NASA Procedural Requirements

NPR 1040.1
Effective Date: July 03, 2003
Expiration Date: July 03, 2008

COMPLIANCE IS MANDATORY

NASA Continuity of Operations (COOP) Planning Procedural Requirements w/Change 1 (03/29/04)

Responsible Office: Office of Security & Program Protection

TABLE OF CONTENTS

Change History

Change #	Date	Description
2	03/30/2005	Definition of vital records changed to be consistent with national level definition as provided in 36 CFR 1236.14.
1	03/29/2004	Deletions made as a result of ADI/Jennings' memo dated 12/05/03. Administrative changes made throughout to correct responsible office codes, names, and to change NPG to NPR.

Preface

P.1 Purpose

a. TEST This NASA Procedural Requirements (NPR) is to provide NASA Management, Center Directors, Chief Information Officers (CIO), Program Managers, and network administrators, with a step-by-step approach to preparing a Continuity of Operations Plan, which addresses long-term losses or disruptions of primary mission-essential operations, supporting facilities, Information Technology (IT) systems, and other essential interdependencies.

b. Required under Executive Order 12656 and Presidential Decision Directives (PDD) 63 and 67, continuity of operations plans provide for a planning and implementation framework that is designed to integrate and expand upon existing emergency preparedness processes established under NPD 8710.1A, Emergency Preparedness Program, NPR 8715.2, NASA Emergency Preparedness Plan Procedural Requirements, and the requirements of the Computer Security Act of 1987 and Office of Management and Budget (OMB) Circular A-130, which will allow the Agency to properly and efficiently address the steps to be taken to maintain its mission-essential operations, or implement transfer of these mission essential operations to alternate location(s), in the event of an emergency event causing long-term contingencies, losses, or disruptions to normal operations.

P.2 Applicability

The provisions of this NPR apply to NASA Headquarters and NASA Centers, including Component Facilities, and to the Jet Propulsion Laboratory (JPL) to the extent specified in its contract.

P.3 Authority

a. 42 U.S.C. 2473(c), Section 203(c)(1) of the National Aeronautics and Space Act of 1958, as amended.

b. Executive Order (EO) 12656, Assignmentof Emergency Preparedness Responsibilities, dated November 18, 1988, as amended.

c. EO 12148, Federal Emergency Management, dated July 20, 1979, as amended.

d. PDD 63, Critical Infrastructure Protection (CIP), dated May 22, 1998.

e. PDD 67, Enduring Constitutional Government and Continuity of Government Operations, dated October 21, 1998.

f. 50 U.S.C. Section 2353.

g. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications

Functions, dated April 3, 1984.

P.4 References

a. PDD 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, dated May 22, 1998.

b. Federal Preparedness Circular (FPC) 60, Continuity of the Executive Branch of the Federal Government at the Headquarters Level During National Security Emergencies, dated November 20, 1990.

c. FPC 65, Federal Executive Branch COOP, dated July 26, 1999.

d. FPC 66, Test, Training and Exercise (TT&E) Program for Continuity of Operations (COOP), dated April 30, 2001.

e. FPC 67, Acquisition of Alternate Facilities for COOP, dated April 30, 2001.

f. National Response Plan.

g. NPD 1040.4, NASA Continuity of Operations.

h. NPD 8710.1, Emergency Preparedness Program.

i. NPR 1620.1, as amended, NASA Security Procedural Requirements.

j. NPR 8715.2, NASA Emergency Preparedness Plan Procedural Requirements.

k. NPD 1440.6, NASA Records Management.

l. NPR 8000.4, Risk Management Procedural Requirements.

m. 40 U.S.C. Section 1441 et seq., Computer Security Act of 1987, as amended.

n. OMB Circular A-130, Management of Federal Information Resources, as amended.

P.5 Cancellation

None

/s/ Bryan O'Connor
Associate Administrator for
Safety and Mission Assurance

CHAPTER 1. Overview of Continuity of Operations Planning

1.1 General

1.1.1 The United States Government policy is that Federal activities have a comprehensive program to ensure the continuity of essential operations under all emergency circumstances (Requirement 30010).

1.1.2 The changing threat environment and lessons learned from accidents, natural disasters, and terrorist incidents, have served to increase awareness of the need for a well thought-out plan of action to ensure the continuity of essential operations across a broad spectrum of emergencies.

1.1.3 As a baseline for preparedness, NASA Headquarters and NASA Centers are required to have in place a viable COOP capability that ensures the performance of their mission-essential operations during any type of emergency, or other situation that may disrupt normal operations (Requirement 30012).

1.1.4 A viable COOP capability must (1) be maintained at a high level of readiness; (2) be capable of being implemented with and without warning; (3) be operational within 12 hours of activation; (4) maintain sustained essential operations for a minimum of 30 days; and (5) take maximum advantage of available field infrastructure, existing Agency emergency preparedness program procedures, and established Information Technology (IT) Security plans (Requirement 30013).

1.2 Continuity of Operation Planning

1.2.1 EO 12656, Assignment of Emergency Preparedness Responsibilities, dated November 18, 1988, as amended, requires that all Federal agencies develop COOP plans to address continuity of mission-essential operations associated with the Agency mission (Requirement 30015).

1.2.2 PDD 63, Critical Infrastructure Protection (CIP), dated May 22, 1998, requires that all Federal agencies develop a comprehensive program for mission-essential assets (operations, facilities, equipment) identification, assessment and planned mitigation of vulnerabilities, and establishment of COOP capability to ensure these assets, when so determined, can continue to operate under all emergency situations (Requirement 30016).

1.2.3 PDD 67, Enduring Constitutional Government and Continuity of Government Operations, dated October 21, 1998, requires that Federal agencies develop, maintain, and implement, when required, the appropriate plans to allow for the continuation of mission-essential agency operations during a time of emergency (Requirement 30017).

1.2.4 The Computer Security Act of 1987 and OMB Circular A-130 require security plans for

Federal Automated Information Systems (Requirement 30018). These security plans include emergency response procedures for information systems to rapidly and effectively deal with the potential disruption of any IT-based mission-essential function.

1.2.5 To avert long-term or disaster scenarios, to minimize their damage, and to ensure continued operational capability, NASA Centers will take proactive steps to develop a COOP for their mission-essential operations (Requirement 30019).

1.3 Goal of Continuity of Operations (COOP) Planning

The goal of COOP is to (1) ensure continuous performance of NASA's mission-essential operations and functions during an emergency situation; (2) protect mission-essential NASA facilities, equipment, vital records, and other assets; (3) reduce or mitigate disruptions to mission-essential operations; (4) reduce loss of life; (5) minimize damage and losses; and (6) resume full, normal essential operations to our customers through a timely and orderly recovery from an emergency.

1.4 Elements of a Viable COOP Capability

1.4.1 All Agency COOP will be developed and documented so when implemented, it will provide for continued performance of mission-essential operations and services under all emergency circumstances (Requirement 30022).

1.4.2 At a minimum, the plan will--

a. Delineate mission-essential operations and functions (Requirement 30024).

b. Establish an order of succession for key leadership positions (Requirement 30025).

c. Identify minimal communications capabilities required to support COOP (Requirement 30026).

d. Identify essential and vital records and databases required to support essential operations and functions, and include steps for protecting them as well as procedures for backup, storage, recycling, and retrieval (Requirement 30027).

e. Outline a decision process for determining appropriate actions in implementing COOP procedures (Requirement 30028).

f. Establish a roster of fully equipped and trained continuity team personnel, with the authority to perform mission-essential operations and functions, and establish procedures for training these personnel in the roles to be performed under COOP implementation (Requirement 30029). Training shall occur on an annual basis (Requirement 30030).

g. Include plans and procedures for employee advisories, alerts, and COOP activation, with instructions for relocation to predesignated facilities, with or without warning, during duty and nonduty hours (Requirement 30031).

h. Provide for personnel accountability and safety throughout the duration of the emergency (Requirement 30032).

i. Provide for attaining functional capability, within 12 hours. (Requirement 30033).

j. Establish reliable processes and procedures to acquire the resources necessary to continue mission-critical essential operations and sustain mission-essential operations for a minimum of 30 days (Requirement 30034).

k. Establish reliable processes and procedures to identify and transition to alternate operational locations if the need arises. (Requirement 30035).

l. Integrate existing emergency preparedness and IT security plans to ensure consistency in overall emergency preparedness program approaches. (Requirement 30036).

m. Provide for annual exercises or tests to ensure viability (Requirement 30037).

1.5 Sensitivity Level of COOP Documents

1.5.1 A Continuity of Operations Plan, as are all emergency preparedness documents, is a "sensitive" document. (Requirement 30039).

1.5.2 A Continuity of Operations Plan is deemed "Administratively Controlled Information (ACI)," and will be handled in accordance with NPR 1620.1, Security Procedural Requirements, as amended. (Requirement 30040).

1.5.3 Electronically stored and distributed copies of the Continuity of Operations Plan must be protected from unauthorized access. (Requirement 30041).

CHAPTER 2. Organization and Assignment of Responsibilities

2.1 Responsibilities

2.1.1 All NASA organizations are responsible for supporting Agency Emergency Response efforts as required by NPD 8710.1, Emergency Preparedness Program; NPD 1040.4, NASA Continuity of Operations; and the COOP Multiyear Strategic and Program Management Plan, developed by the Agency COOP Program Executive Coordinator, which will define explicitly the ways and means to--

a. Support implementation of EO's 12148 and 12656, and PDD's 63 and 67 (Requirement 30044).

b. Coordinate with Headquarters and Center Senior Management for additional resources when the situation dictates (Requirement 30046).

c. Provide Center Management with the means to appropriately staff COOP teams to make the COOP operational (Requirement 30047).

2.2 The NASA Administrator

The NASA Administrator or Designeewill appoint an Agency COOP Program Executive Coordinator from the Office of Safety and Mission Assurance with sufficient authority to ensure that the COOP process is included as an integral part of the Agency's core mission of safety and mission assurance (Requirement 30048).

2.3 The Agency COOP Coordinator

The COOP Coordinator is responsible for--

2.3.1 Developing a COOP Multiyear Strategy and Program Management Plan (Requirement 30050).

2.3.2 Coordinating with designated Center COOP Coordinators for the development of COOP procedures for Headquarters, individual Centers, and subordinate organizations, as applicable, which provide for the following:

(1) Evaluation of Agency mission-essential infrastructure, functions, facilities, and other essential interdependencies for consideration for COOP (Requirement 30052).

(2) Predetermined delegations of authority and orders of succession (Requirement 30053).

(3) Contingency staffing to perform mission-essential operations. (Requirement 30054).

(4) Alternate operating facilities, as required (Requirement 30055).

(5) Interoperable communications, information processing systems, and equipment (Requirement 30056).

(6) Protection of vital records and systems (Requirement 30057). See definition of vital records and systems in Chapter 5, Glossary of Terms, Abbreviations, and Acronyms.

2.3.3 Coordinating exercises, tests, and training, of Agency COOP, to include COOP contingency staffs, and essential systems and equipment, to ensure timely and reliable implementation of COOP Procedures (Requirement 30058).

2.3.4 Participating in periodic interagency COOP exercises to ensure effective interagency coordination and mutual support (Requirement 30059).

2.3.5 Coordinating intra-Agency COOP efforts and initiatives with policies, plans, and activities related to antiterrorism established under PDD 62 and Critical Infrastructure Protection established under PDD 63 (Requirement 30060).

2.3.6 Ensuring that COOP documentation is managed in accordance with NPD 1440.6, NASA Records Management, (e.g., collect and store all vital records, such as personnel, pay, mission program data, emergency operations plans, facility engineering design plans and drawings) and provide for assistance to other NASA Centers in postdisaster recovery of vital records, where applicable (Requirement 30061).

2.4 Center Directors

Each Center Director is responsible for--

2.4.1 Appointing a Center COOP Coordinator (Requirement 30063). The Center COOP Coordinator should be a senior staff member from either the CIO or Emergency Services organization.

2.4.2 Emphasizing emergency preparedness and COOP readiness as part of the Center's core mission. (Requirement 30064).

2.4.3 Ensuring Center Chief Financial Officers (CFO) provide necessary assistance to COOP activity (Requirement 30065).

2.5 Chief Information Officers (CIO)

The CIO's are responsible for--

2.5.1 Ensuring Agency IT systems have the appropriate security and contingency plans, as required under OMB Circular A-130 (Requirement 30067).

2.5.2 Ensuring Special Management Attention (SMA) systems are evaluated for COOP (Requirement 30068).

2.6 Center COOP Coordinator

Each Center COOP Coordinator is responsible for--

2.6.1 Coordinating the development and consolidation of all COOP for their select minimum essential infrastructure assets, within their respective Center, in accordance with requirements

established in this NPR and established emergency preparedness plans (Requirement 30070).

2.6.2 Coordinating with the Agency COOP Coordinator and individual organizational management, scheduling, and overseeing yearly training and exercises, as required (Requirement 30071).

2.6.3 Coordinating tenant organization COOP development, as appropriate (Requirement 30072).

2.7 Program Management

The Program Management is responsible for--

2.7.1 Ensuring the development, implementation, maintenance, and testing of COOP, when required, in accordance with the requirements in this NPR and other references (Requirement 30074).

2.7.2 Coordinating all program COOP activity with the Center COOP Coordinator (Requirement 30075).

2.7.3 Ensuring that program COOP is included in organization budget activity (Requirement 30076).

2.8 Chief Financial Officers (CFO)

The CFO's are responsible for--

2.8.1 Establishing a COOP funding mechanism (Requirement 30078).

2.8.2 Assisting Center management on COOP budget development (Requirement 30079).

2.8.3 Providing systems that will account for COOP expenditures (Requirement 30080).

2.9 Vital Records Managers

The Vital Records Managers are responsible for--

2.9.1 Ensuring that local policies and procedures are developed and implemented for the identification, designation, protection, and retrieval of Center vital records in accordance with NPD 1440.6, NASA Records Management, and other governing requirements (Requirement 30082).

CHAPTER 3. Continuity of Operations Planning (COOP) Process

3.1 General

3.1.1 COOP involves more than planning for a move offsite if a disastrous event destroys or disrupts a mission-essential operation, function, facility(ies), supporting IT system(s), or other interdependent essential infrastructure, on which the mission-essential operation depends.

3.1.2 COOP must also address how to keep an organization's mission-essential operations and supporting systems operating in case of long-term disruptions.

3.2 NASA COOP Criteria

3.2.1 To ensure that the Agency's critical operations are thoroughly reviewed for COOP consideration, Centers will assess Agency Mission Essential Infrastructure (MEI), supporting operations, and other interdependencies, and evaluate that infrastructure from a risk to the national welfare perspective, which by themselves or as a result of a Memorandum of Understanding, or other agreement with another Federal agency, must continue to operate or remain capable to operate at the primary or an alternate location under all emergency circumstances (Requirement 30088).

3.2.2 Center MEI inventories will be identified and maintained by the Center Critical Infrastructure Assurance Office (CIAO) per requirements found in NPR 1620.1, NASA Security Procedural Requirements, as amended (Requirement 30089).

3.2.3 Centers will use the following criteria when making COOP judgments (Requirement 30090). These criteria will serve to identify essential operations that require development of COOP:

a. Would the loss of a Center MEI capability or operation compromise national security?

b. Would the loss of a Center mission-essential infrastructure capability or operation

have an immediate and significant adverse effect on the health and safety of the general public at large?

c. Is a NASA Center mission-essential capability or operation critical to the performance of another agency's COOP essential operations and required, by agreement, to remain viable, without interruption, under all emergency conditions?

d. Is the NASA mission-essential capability or operation regulated, legislated, or directed by Executive order to operate under all emergency scenarios?

e. Is the mission-essential capability or operation tied into a space exploration vehicle and equipment command and control operations that if rendered inoperable, would place personnel, vehicles and/or equipment at risk?Would the cost to recover from such an event exceed NASA's budget capability?

f. Is the mission-essential capability or operation a deemed vital service, as determined by NASA management and, therefore, required under COOP?

3.2.4 The ability for NASA's Senior Management to continue to manage the Agency and individual Centers during a disastrous event is inherently critical to NASA and the U.S. Government. Essential management operations will be included under a COOP (Requirement 30091).

3.2.5 NASA assets identified as MEI which may, due to their size, configuration, and age, be difficult and expensive or impractical to relocate to an alternate facility or rebuild if destroyed (e.g., wind tunnels, Local Area Network (LAN), Wide Area Network (WAN)). They should be carefully evaluated under COOP criteria to ensure that all aspects of their criticality and replaceability are thoroughly considered, before establishing a COOP (Requirement 30092).

3.3 Continuity of Operations Planning Process

3.3.1 Evaluation of Identified Mission-Essential Operations

a. The evaluation of an organization's MEI operations generally centers around the organization's business plan.

b. Because the development of the business plan is used to support the continuity of operations planning process, it is necessary, not only to ensure accurate evaluation of essential operations and business processes, in accordance with criteria established in paragraph 3.2, but also to set priorities and time criticalities for them.

c. The Program Manager and staff are responsible for ensuring the completion of the business plan and for prioritizing the resumption, recovery, or restoration needs for the organization's mission-essential operations, if any (Requirement 30097).

d. Because a fully redundant capability for each function is prohibitively expensive for

most organizations, certain operations will not be performed in case of a disaster.

e. If appropriate priorities have not been set, it could make a difference in the organization's ability to survive a disastrous event.

f. Development of a Mission Statement.

(1) Government departments, divisions, and offices generally have a formal statement concerning the mission(s) to be performed (Requirement 30101).

(2) These statements may be contained in organization policies or directives, handbooks, or public information guides.

(3) Regardless of the source, the criticality determination process starts with an overall mission statement that identifies what the organization is responsible for doing.

g. Functional Activities Listing.

(1) The process continues by developing a list of all operations performed by the office in support of the essential mission.

(2) In parallel with this listing, it is also necessary to identify those operations that are dependent on specialized support (such as IT Systems, communications, certain data or records, physical infrastructure, human resources) as well as the extent of that dependency (i.e., is the function totally dependent on a particular type of support, is only some portion that can be quantified dependent on such support, or could the function be performed manually with little or no loss of efficiency) (Requirement 30106).

(3) See Paragraph 3.3 for a more detailed discussion of specialized support resources.

(4) Any special requirements affecting the performance of the function or relating to the information involved should also be noted.

(5) These could include the sensitivity of data, or whether there is a specific timeframe when data are more critical than other times.

(6) See Appendix A, for guidance on how to perform this critical step and Tab A, which contains an Office Mission and Functionality Matrix template that is designed to aid in this definition process.

h. Criticality Matrix (Requirement 30111).

(1) The next element is the development of a criticality matrix.

(2) Criticality guidelines must be developed which identify those office operations that deal with aspects that are critical to any Government agency, and the timeframes that must be associated with those factors (Requirement 30113).

(3) Developing a matrix, similar to that used for determining sensitivity and protection

requirements in system security plans, is one approach to determining criticality.

(4) Most NASA offices and operating Centers are not involved with the more obviously critical factors, such as saving lives or national defense.

(5) They must develop an office-specific list of critical operations (Requirement 30116).

(6) The primary objective is to identify only those mission-essential operations that, if not performed, will cause the greatest loss to the office in terms of inability to operate and the expenditure of additional funds.

(7) Reserved.

(8) These guidelines should permit each function to be evaluated in terms of the importance of the function in accomplishing the mission of the office and how quickly this function must be performed.

(9) The longer the function can do without specialized support, the less critical is the specialized support, hence criticality is a function of time.

(10) See Appendix A for guidance on how to perform these critical steps and Tabs B and C for sample Criticality Factors and Timeframes and Office Function Criticality Matrix that are designed to aid in this process.

i. Criticality Determination (Requirement 30122).

(1) The next part of the process is to compare the functional activities against the criticality determinations and corresponding timeframes.

(2) A COOP is concerned with all mission-essential operations and goes beyond those functions requiring only IT processing and operations.

(3) All office operations are compared against the criticality determinations and time factors, and against each other.

(4) The result is a prioritized list of mission-essential activities, based on criticality, and reflected in terms of the maximum timeframe that these essential operations are not performed before the organization fails to accomplish its mission.

3.3.2 Identification of Resources, Vital Records, and Interdependencies that support NASA's Mission-Essential Operations.

a. After essential missions and business operations are identified, support resources and vital records must be identified, as well as the timeframes in which each resource is used and the effect of unavailable resources on the essential operations in support of the mission (Requirement 30124).

b. It is important to note that the COOP resources inventory must consist of only those

physical resources, vital records, and support services necessary for an office and organization to perform the essential parts of its mission (Requirement 30125).

c. The COOP does not provide for the immediate or even eventual replacement of all existing resources at an alternate site. Rather, it is intended to implement a viable and effective essential function in an alternate location for a minimum of at least 30 days.

d. In addition to precisely identifying the minimum levels of resources required to activate a temporary office, the resources inventory must also identify who is responsible for each category of items, where the existing items are located, (and if backup supplies already exist, where they are located, and in what quantity), what and where is the source of replacement or resupply, and in some instances, what is the cost and timeframe for replacement (Requirement 30127).

e. As COOP progresses, preparatory actions will drive the modification or expansion of certain inventory data.

f. Continuity of operations planning should address all the resources needed to perform an essential function, including:

(1) Human Resources (Requirement 30130).

(a) Human resources requirements include essential management staff, operational and support personnel, systems users, and security personnel.

(b) Some essential operations require personnel with special expertise or training, while others require lesser skill levels.

(c) Security is especially critical when potential for continuous protection of a vacated site, and protection of an alternate site need to be considered simultaneously.

(d) Additionally, the human resources aspect of continuity of operations planning includes establishment of plans of succession and Delegations of Authority (DOA) for both Headquarters Operations and individual Centers.

(e) COOP planners will also consider Plans of Succession and DOA for each organization, program, or project operating under a COOP.

(2) Processing Capability (Requirement 30131).

(a) Traditionally, contingency planning has focused on processing power.

(b) Although the need for data backup remains vital, today's other processing alternatives are also important.

(c) LAN's, microcomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

(3) Automated Applications and Data (Requirement 30132).

(a) NASA information systems run applications that process all types of data, run all types or programs, and reach far into space.

(b) Without current electronic versions of both vital applications and data, computerized processing may not be possible.

(c) If the processing is being performed on alternate hardware, the applications must be compatible with the primary hardware, operating systems and other software (including version and configuration), and numerous other technical factors.

(4) IT-Based Services (Requirement 30133).

(a) NASA uses many different kinds of IT-based services to perform most, if not all, of its essential and nonessential operations and functions.

(b) The two most important IT services are normally communications services and information services.

(c) Communications can be further categorized as data and voice and in some instances, satellite.

(d) However, in many Centers these may be managed by the same service. Information services include any source of information outside of the organization. Most of these sources are automated, including Online Government and private databases, the Internet, and external e-mail.

(5) Secure Communications (Requirement 30134).

(a) COOP will include the development and implementation of secure communications capability for key personnel, when appropriate.

(b) COOP will include hard-wire and wireless capability, requirements and procedures for use, pre-event purchase and deployment, familiarization, and training.

(6) Communication with Key Government Officials.

(a) COOP must be developed and properly coordinated to ensure communications capability with key Government Officials (e.g., The President, The Vice President, National Command Authority (NCA), Department of Homeland Security), and others as necessary, which may be effected by the NASA Administrator during an emergency event affecting the Washington, DC, area, resulting in mass evacuation of Government agencies, or under any other emergency situation in which key personnel of the Federal Government may become widely dispersed and require dependable and secure modes of communication with the executive branch (Requirement 30135).

(7) Telecommunications Service Priority (TSP) Program (Requirement 30136).

(a) The TSP Program is a Federal Communications Commission (FCC) program used to identify and prioritize telecommunication services that support National Security or Emergency Preparedness (NS/EP) missions.

(b) The TSP Program also provides a legal means for the telecommunications industry to provide preferential treatment to services enrolled in the program.

(c) Center organizations establishing COOP capability should consider participation in the TSP Program, where appropriate.

(8) Physical Infrastructure (Requirement 30137).

(a) Physical infrastructure elements include a safe working environment and appropriate equipment and utilities.

(b) This can include office space, heating, cooling, venting, power (including determining the need and source of uninterrupted power), water, sewage, other utilities, desks, fax machines, personal computers, terminals, courier services, file cabinets, and many other items.

(c) In addition, computers also need space and utilities, such as electricity, communications lines (connectivity). Electronic and paper media used to store applications and data may also have specific physical requirements.

(9) Vital Records, Documents, and Papers (Requirement 30138).

(a) The performance of many NASA operations relies on vital records and various documents, papers, or forms.

(b) These records could be important because of legal need, or because they are the only record of the information.

(c) Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

(10) Appendix B contains a Critical Resources Inventory Outline that may be used to assist in the identification of critical resources.

(a) Also see Appendix B for sample tables for a methodology of matrixing this information.

(b) As shown in the sample tables, the "QTY 1, QTY 2, QTY 3," fields can be used to identify the quantity of personnel, services, supplies, and equipment needed as the criticality timeline continues.

(c) This will also aid in budgeting for a period or coverage to ensure that a percentage of the resources are available when needed.

3.3.3 Establishment of Delegations of Authority (DOA)

a. To ensure rapid response to any emergency situation requiring COOP implementation, DOA's should be preestablished to enable designated personnel to make the appropriate policy determinations at the Headquarters, Centers, and other organizational levels, as deemed appropriate (Requirement 30141).

b. These DOA's should be included as an appendix to the Continuity of Operations Plan and the following: (Requirement 30142).

(1) Identify the programs and administrative authorities needed for effective operations at all organizational levels having emergency responsibilities.

(2)Identify the circumstances under which the authorities would be exercised.

(3) Document the necessary authorities at all points where emergency actions may be required, delineating the limits of the authority and accountability.

(4) Clearly state the authority of designated successors, to exercise Agency direction, including any exceptions, and the successor's authority to redelegate operations and activities, as appropriate.

(5) Indicate the circumstances under which the delegated authorities would become effective and when they would terminate.

(6) Ensure that officials who may be expected to assume authorities in an emergency are trained to carry them out.

(7) Be appropriately updated upon transfer, termination, or other personnel action resulting in the individual's departure.

3.3.4 Plans of Succession (POS)

a. NASA Headquarters and individual Centers will establish, promulgate, and maintain POS to key positions (Requirement 30144).

b. POS are an essential part of NASA's COOP activity and will be included in the COOP plan as an appendix (Requirement 30145).

c. POS will be sufficient in depth to ensure NASA's ability to perform essential operations while remaining a viable part of the Federal Government during any emergency (Requirement 30146).

d. Geographical dispersion is essential, consistent with the requirement for ensuring appropriate succession to office in emergencies of all types.

e. Each principle NASA activity will, as appropriate (Requirement 30148).

(1) Establish POS to the position of NASA Associate and Assistant Administrators.

(2) Establish POS to other key Headquarters leadership positions.

(3) Establish POS for each Center.

(4) Identify any limitations of authority based on DOA's to others.

(5) Describe POS by positions or title, rather than names of individuals.

(6) Include the POS in the vital records inventory of the Agency and Center.

(7) Revise POS as necessary and distribute revised versions promptly as changes occur.

(8) Establish the rules and procedures that designated officials are to follow when facing the issues of succession to an office in emergency situations.

(9) Include in succession procedures the conditions under which succession will take place, method of notification, and any temporal, geographical, or organizational limitations of authorities.

(10) Assign successors to the extent possible among emergency teams established to perform essential operations, to ensure each team has an equitable share of duly constituted leadership.

(11) Conduct orientation and training programs to prepare successors for their emergency duties.

3.3.5 Anticipation of Potential Contingencies or Disasters.

a. Although it is impossible to anticipate everything that can go wrong, this step involves identifying a likely range of problems.

b. Developing scenarios can help an organization to prepare a plan that addresses a wide range of possible mishaps.

c. COOP planners must consider that the hanging-threat environment, including military or terrorist attack-related incidents, have shifted awareness to the need for COOP capabilities that enable NASA to continue its mission-essential operations across a broad spectrum of emergencies.

3.3.6 Selection of Continuity of Operations Planning Strategies.

a. When strategies are developed and evaluated, existing controls for preventing and minimizing losses should be considered.

b. Because no one set of controls can prevent all losses in a cost-effective manner,

prevention and recovery efforts should be coordinated.

c. Risk assessments, conducted by the COOP management team, can also help determine an optimal strategy.

d. A COOP strategy normally consists of five parts: prevention, response, resumption, recovery, and restoration of services or operations:

(1) Prevention refers to those measures taken to forestall a disruption of service, (e.g. preventive maintenance, virus prevention, physical and/or procedural security measures as developed under the Agency Critical Infrastructure Protection Program).

(2) Response encompasses the initial actions taken to protect lives and limit damage.

(3) Resumption refers to the steps taken to continue support for critical operations.

(4) Recovery concerns the reactivation of a greater scope of business processes and services beyond the most time-sensitive processes.

(5) Restoration is the return to normal operations.

e. The longer it takes to restore normal operations, the longer the organization will have to operate in the resumption or recovery mode.

f. The selection of a strategy needs to be based on practical considerations, including feasibility and cost.

g. Different categories of resources should also be considered.

3.3.6.1 Human Resources.

a. During a major continuity plan implementation, people will be under significant stress and may panic.

b. If the continuity plan is implemented as a result of a local or regional disaster, their first concerns will probably be their family and property.

c. In addition, many people will be either unwilling or unable to come or remain at work, or travel to an alternate site to assist in resumption of operations.

d. Cross-training of employees inside and outside the affected organization is one way to ensure availability of sufficient personnel to assist in maintaining essential mission capability.

e. Additional hiring or temporary services are also available but should be carefully considered and weighed against any possible security vulnerabilities.

3.3.6.2 IT Processing Capability.

a. For mission-essential operations that rely heavily on IT support, less serious events

involving short-term disruptions, processing capabilities can be restored from backups or original media, by repairing equipment components, or by purchasing new equipment.

b. Federal agencies have the authority to issue purchase orders to quickly acquire needed equipment and supplies in limited quantities.

c. This authority is usually limited but is sufficient to acquire Commercial Off-The-Shelf (COTS) hardware and software.

d. Essential hardware could be acquired by purchase orders in one of two ways, purchase of replacement or upgraded equipment or lease of essential equipment for a limited period of time.

e. The outright purchase of identical replacement hardware is the most obvious use of the purchase order option.

f. However, the purchase of upgraded equipment is a reasonable alternative, given the fact that the existing equipment may not be economically salvageable.

g. On the other hand, the short-term lease of essential equipment to augment or temporarily replace existing equipment during salvage operations provides a cost-effective alternative.

h. There is, however, a risk involved with the leasing of equipment that must be addressed for long-term events under a COOP. That risk is the fact that those systems must be thoroughly scrubbed prior to deployment to ensure they are free of infected hardware and software and in preparation for return to the vendor to ensure the integrity and protection of information that has been stored or processed on the machines.

i. Although these two options could offset the lack of facilities and equipment at the time of the disaster, they are subject to the disadvantages of high cost and long preparation time.

j. In a widespread disaster, the requirements for space, hardware, communications, could temporarily exceed demand.

k. These two options must also be used in combination because neither provides for facilities (to include associated utilities and communications) and equipment, furnishings, and supplies.

l. For less serious events involving short-term disruptions, the COOP defers to the use of in-house contingency plans developed under the auspices of the Center Emergency Preparedness Program or IT Security Plans, developed under the requirements of OMB Circular A-130.

m. For a more serious continuity event, however, the strategies for ensuring

operational capability are normally grouped in five categories:

(1) Category 1. Hot Site. A hot site is a building already equipped with processing capability and other services.

(a) Operational standby facilities require a subscription contract and charge various fees.

(b) Normally, a 3- or 5-year contract is negotiated and includes a specific hardware and software configuration with detailed communications requirements, which must be updated whenever changes occur. Subscription fees are determined by these requirements.

(c) The reduction in costs for the minimum essential capabilities required by a COOP is not significant and may not be warranted for continuity of operations.

(d) Another potential drawback for the IT user is that these services are relatively new and not widely dispersed.

(e) Therefore, a Hot Site facility may not be conveniently located.

(2) Category 2. Cold Site. A Cold Site is a building for housing alternate operations and/or processors that can be easily adapted for use.

(a) Such a facility may be owned by NASA, situated at a NASA Center, owned by another Government agency (e.g., DOD, GSA), or Government-leased for one or more organizations.

(b) In the event of a disastrous event, the affected office(s), in conjunction with hardware vendors, acquires and installs the essential IT hardware, software, and communications.

(c) Cold Sites are more practical for IT-based operations since a shell facility may be owned by NASA or the facility can be virtually any office space with sufficient electrical power, communications line capability (installed or capable of being installed during a disaster situation), and regular air conditioning.

(d) IT hardware is more readily available, more easily shipped, and more easily installed.

(e) A Cold Site may also be supported by a special equipment contract (if not already in place as part of a standard hardware maintenance agreement).

(f) There are a number of hardware vendors who offer guaranteed delivery and setup within 24-hours.

(g) Although the maintenance costs are somewhat less than an operational standby, they represent a continuing expense.

(h) For IT activities, consideration should be given to leasing essential IT equipment and peripherals to augment equipment salvage from the primary site or to temporarily replace essential hardware until the primary site can be restored without additional disruption to IT configuration.

(i) Leasing eliminates the ongoing maintenance costs of a special equipment contract but does not provide for the guarantees that appropriate equipment will be available when needed or within required timeframes.

(j) As described earlier, leasing also creates the problem of data security, as special precautions must be taken to ensure that all data that has been stored or processed on the system have been removed from the leased equipment.

(k) This practice requires more than a simple deletion of the data as deleted files can still be detected, identified, and restored.

(l) The site availability timeframe, which includes hardware, communications, and equipment installation, may not meet organizational or system requirements as set forth in continuity plans.

(3) Category 3. Redundant Site. A redundant site is a site that is equipped and configured exactly like the primary site.

(a) It is either operating in parallel with the primary site or can be activated at a moment's notice.

(b) A redundant site is critical in situations where the operational reliability of the asset is 100 percent and cannot be interrupted for any length of time.

(4) Category 4. Reciprocal Agreement. A reciprocal agreement is a formal agreement that allows two organizations to back up each other.

(a) The agreement is usually with an external organization, for the two to provide backup IT processing support to one another in the event of a disruption in primary processing support.

(b) The external office, division, or directorate is not in the business of providing IT support, but agrees to provide reciprocal support in recognition of mutual backup requirement.

(c) Although low development and maintenance costs are the principle advantage to this alternative, consideration must be given to establishing an agreement with an organization that will not be affected by the same disaster.

(d) Reaching an agreement with another activity, such as a counterpart office in another division or operating Center, provides no effective continuity of operations

capability if that activity is affected by the same disaster.

(e) The activities establishing a mutual assistance agreement should be geographically separated.

(f) The biggest disadvantage of mutual assistance agreements is that, "Their disaster becomes your disaster."

(g) Many of the disadvantages noted above identify areas of hardship and general inconvenience to both activities.

(h) Without a specific mission-essential operation, required staffing, supporting specialized services (e.g., IT system, site, other interdependencies), and pair of organizations in mind, it is difficult to evaluate a mutual-assistance agreement alternative completely and fairly.

(i) Mutual-assistance agreements are not considered viable solutions without a formal agreement outlining all conditions and signed by individuals in positions of authority to uphold the agreement.

(5) Category 5. Hybrids. Any combinations of the above, such as having a Hot Site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

(a) In addition to these five alternatives, another approach readily available to mission-essential operations dependent on IT environments, is to allow key staff to work at home (telecommute) during the emergency event.

(b) Even limited use of this alternative could ease the continuity of operations burden by reducing or eliminating the need to provide suitable office space and to acquire hardware and/or software assets.

(c) In addition to reduced costs, it offers the advantage of immediate availability.

(d) It can also serve to reduce the level of anxiety staff may experience if separated from their families during the event.

(e) It can be thoroughly tested; however, there are also disadvantages.

(f) The event may be so widespread as to have disrupted service in a region as opposed to local area.

(g) Also, technical and maintenance support to privately owned property poses legal difficulties and limits sustainability, while information security and anti-viral protection could become issues requiring well thought-out solutions.

(h) Use of Government-owned IT equipment for use at home, or the requirement for designated personnel to take home issued laptops on a daily basis, could reduce legal

and operational concerns.

Figure 1 presents a set of evaluation characteristics that may be used to help weigh the alternatives for determining alternate site operational and processing capability.

Evaluation Characteristic	Planning Considerations
Compatibility	Hardware, software, and communications that are or would have to be installed at an alternate site must be the same as or compatible with original equipment supported.
Accessibility	The alternate site must be readily accessible, but not so close as to share the same disaster.
Reliability	The alternate site must be capable of supporting the operations of the affected office(s) 24 hours a day, 7 days a week. Maintenance for site equipment, hardware, and communications should be on-site or on-call.
Capacity	The alternate site and facility and computer equipment must have sufficient floor space, heating, cooling, and power (including uninterrupted power when required), communications lines, and memory capacity to support the number of staff and suite of equipment required.
Security	Physical security at the alternate site must be sufficient to protect personnel, property, and the sensitivity of the information and data. Security assessments will need to be conducted by assigned security personnel.
Time to prepare	There must be sufficient time to prepare for the disaster, including time to prepare and convert data and software; prepare the site; prepare and store supplies, forms, and documentation; obtain and install power and communications circuits; and prepare and test the COOP.

Support and assistance	There must be on-site technical support and assistance to set up and configure the hardware, software, and communications.
Cost	Cost factors can be subdivided into three categories: • Preparation costs include cost of any equipment or LAN/WAN. • Maintenance costs include hardware, software, or telecommunications maintenance and lease fees. • Execution costs are incurred in declaring a disaster and executing the COOP, including rent, travel, and per diem.

Figure 1. Processing Capability Evaluation

3.3.6.3. Automated Applications and Data

a. Normally, the primary contingency or continuity strategy for applications and data is regular backup and secure offsite storage.

b. Important issues to be addressed include the frequency of backups, the frequency of offsite storage, and the manner of transporting backups.

c. Office policy should require IT or LAN administrators to maintain separate master copies immediately upon implementation of approved changes, store the masters in a secure offsite location, together with copies of all applicable hardcopy documentation and operating manuals.

d. A similar policy should require the appropriate individual(s) to prepare backup copies of all electronic files on a regular (e.g., not less than weekly) basis, to maintain copies of all required references and hardcopy files, and to store the backup copies in a secure offsite location.

e. In the IT environment, the volume of equipment and supplies to be stored is relatively small, based on the nature of the media involved (diskettes, 8 mm cartridge tapes, CD's).

f. Headquarters and individual Center Data Centers and operational LAN's/WAN's make provisions for storing of these types of materials in support of Agency activities.

g. Hardcopy data could be stored on a permanent retention basis in local agency, Center, or general Federal storage facilities.

3.3.6.4. IT-Based Services.

a. Communications is also a key discriminator in selecting an appropriate COOP alternative.

b. Incompatible communications or insufficient lines may disqualify a site or option.

c. The COOP planner must ensure that adequate compatible communications are available at the alternate site or that they can be provided during a disaster situation.

d. As appropriate, an agreement with a communications vendor must be negotiated. This agreement must cover all necessary voice, data, and image communications.

e. Separate agreements must also be negotiated with equipment vendors for modems, fax machines, telephones, encryptions devices, and keys, if required.

f. Service providers may offer contingency services.

g. Voice communications carriers often can reroute calls to a new location, and data communications carriers can also reroute traffic.

h. Local voice service may be carried via cellular phones.

i. If one service is down, it may be possible to use another.

j. Resuming normal operations may require rerouting of communications.

3.3.6.5. Physical Infrastructure.

a. Arrangements must be made for office space, furniture, data and communications processing capability, other support, and more, as applicable.

b. If the COOP calls for moving offsite to an alternate facility, procedures need to be developed to ensure a smooth transition back to the primary facility or to a new permanent location.

c. A related alternative available to Federal agencies is the U.S. Government's procurement system.

d. The General Services Administration (GSA) has the responsibility of assisting agencies in acquiring additional office space on an "as required" basis for Federal agencies, and the responsibility of managing standing contracts for goods and services. See Federal Response Plan, 9239.1-PL.

e. Because minimal space is required for continuity of operations activities, this capability permits fairly rapid acquisition of space without the "overhead" costs of rents or subscription fees.

3.3.6.6. Vital Records, Documents, and Papers.

a. The primary contingency strategy is usually backing up into magnetic, optical, microfiche, or other medium and offsite storage.

b. Copies of such records should be cycled on a schedule to be determined by the organization to ensure that the copies are current and acceptable.

c. A supply of forms and other needed papers can be stored offsite as well.

d. Backup storage space should be located close enough to the primary site for convenience in placing items into storage on a regular basis, but not so close that it will be affected by the same disaster.

e. Onsite (i.e., same office and building) storage is not recommended.

3.3.7. Documenting Continuity of Operations Planning Strategies.

a. With continuity of operations strategies well defined, the next step is to create the COOP itself.

b. The COOP needs to be written, kept up-to-date as the organization, systems, and other factors change, and stored in a safe place.

c. A written plan is critical during a continuity of operations event, especially if the person who developed the plan is unavailable to assist in its implementation.

d. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan.

e. It is generally helpful to store up-to-date copies of the COOP in several locations, including any offsite locations, such as alternate processing sites or backup data storage facilities. The structure of the COOP includes:

(1) Plan Overview - consists of an introduction, statement of policy, objectives, scope, assumptions, recovery strategy, and plan administration responsibilities.

(2) Continuity Process Overview - outlines the four major stages of the process, after prevention (emergency response, resumption, recovery, and restoration), including the central activities and objectives of each stage, and the relationships among stages.

(3) Continuity Team Organization - defines the specific organization set up to work towards survival and the resumption of time-sensitive essential operations. The teams associated with this plan represent office functional units and/or support operations developed to respond, resume, recover, or restore operations of the facility and/or system. Each team is comprised of individuals with specific responsibilities or tasks that must be completed to fully execute the plan. The organization will be based upon the emergency incident command structure established by the National Interagency Incident Management System (NIIMS). Figure 2 below, presents a representative example of a Continuity Team Organization structure.

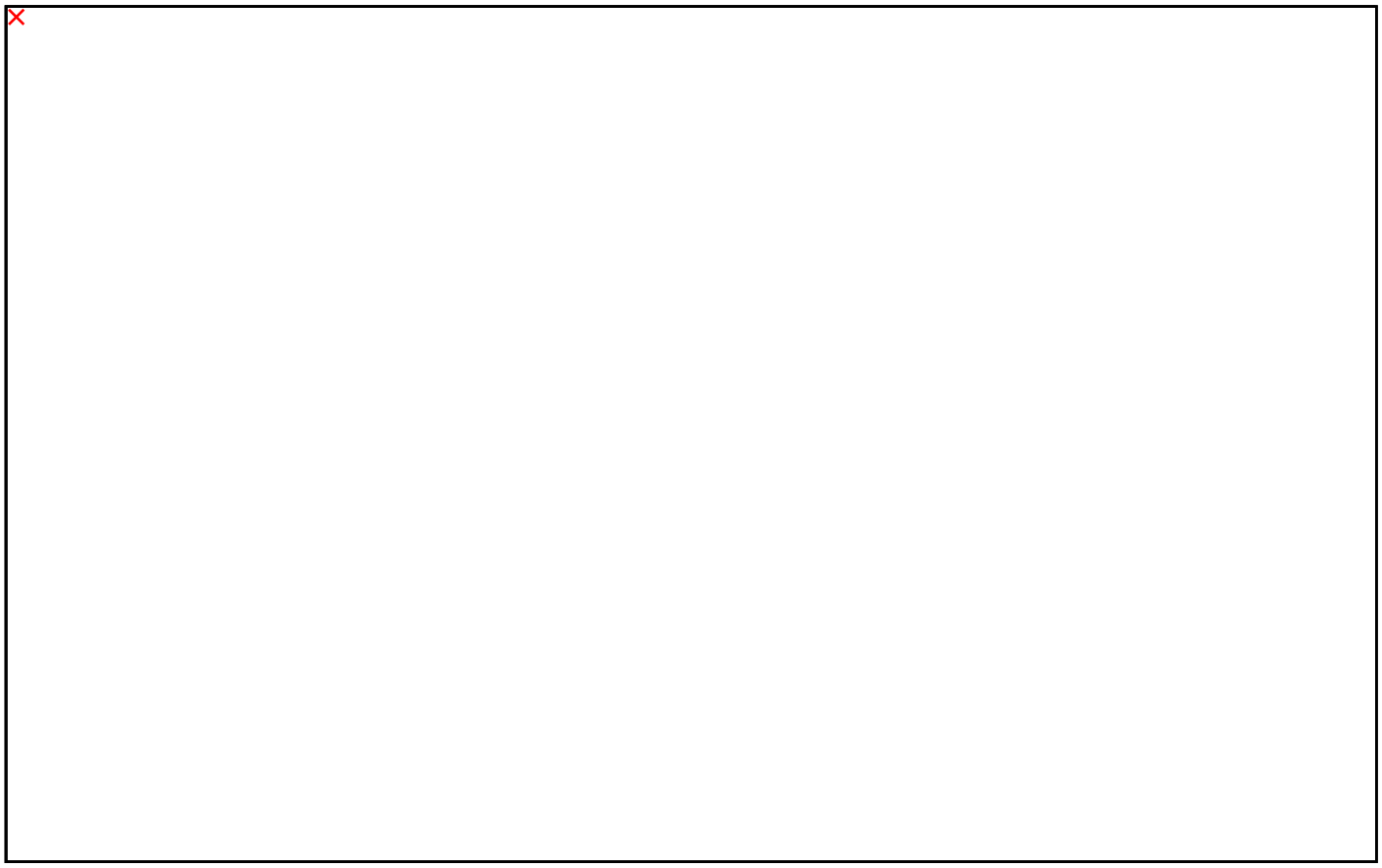

Figure 2. Representative Continuity Team Organization Structure

(4) Plan Maintenance - includes both scheduled and unscheduled maintenance, as well as periodic reevaluation process. Scheduled maintenance consists of quarterly reviews and updates, as well as annual structured walk-through and/or tactical exercises (as described in the Plan Exercise section below). The purpose of the plan review is to determine whether changes are required to strategies, tasks, procedures, the continuity organization, and notification procedures. The majority of unscheduled maintenance activities occur as a result of major changes to service level agreements, hardware configurations, networks, and production processing. The Continuity Plan maintenance process should also include a periodic reevaluation of the minimum hardware capacity required to provide short-term response, resumption, recovery, and restoration capability. The reevaluation process must address the capacity growth requirements associated with the increase of transaction processing volumes of the production application systems, as well as the addition of new systems to the production environment.

(5) Plan Exercise - consists of the various types and scope of exercises designed to test and evaluate the COOP. Exercises should be conducted not less than annually, and when a COOP has been implemented, major revision to the plan has been completed,

when additional systems or requirements are implemented, when significant changes in systems, applications and/or data communications have occurred, and when the preparedness level of continuity teams must be verified. An exercise may include structured walk-throughs, tactical exercises, live production exercises, simulations, and announced and unannounced exercises.

(6) Plan Execution - details for plan execution reside in the Appendices to the COOP itself. These Appendices contain specific data required by the various teams to perform their designated roles during each stage of the process. Appendices include--

(a) Priority Contact List - includes employee names and contact information.

(b) Employee/Contractor Notification List - contains a directed list of who is to contact who regarding the communication of continuity information.

(c) Team Member Roster - identifies the specific individuals belonging to each Team and their contact information.

(d) Team Task List with Dependencies - consists of detailed, step-by-step listing of each task to be performed by the members of the various continuity teams. Where a specific task must await action by a member of another team, this is so noted, and the task and responsible individual is identified. This area is key to the entire COOP.

(e) Enterprise Process Configuration - lists, for each IT system or process, the associated software, equipment, supplies, network information, and responsible teams.

(f) Vendor Representatives - contains a listing of all applicable vendor contact information, including local representatives and focal points within the organization.

(g) Location Information - contains the location of all offsite storage, alternate operating locations (Hot or Cold Sites), record repositories. Driving or transportation instructions and personnel focal point contact information is also included for each location.

(h) Vital Records - includes a listing of all necessary emergency operating documents, manuals, diskettes, CD-ROMS, and all other media necessary to implement the COOP. Additionally, this includes appropriate personnel, legal, and financial records that if lost would seriously impact the Agency, Center, and organization's capability to conduct mission-essential operations, and in some cases, seriously impact recovery and resumption of normal operations.

3.3.8. Test and Revise Strategy.

a. A COOP should be tested to train personnel and to keep the plan in step with changes to the operating environment.

b. The extent and frequency of testing will vary among organizations, systems, and

particular mission.

c. There are several types of testing--

(1) Review: This is a simple test to check the accuracy of the COOP. For instance, a reviewer can check the accuracy of contact telephone numbers, building and room numbers, and whether the listed individuals are still in the organization.

(2) Analysis: An analysis may be performed on the entire plan or parts of it. The analyst may mentally follow the strategies in the COOP and look for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to detect missing or unworkable pieces of the plan.

(3) Simulation and Test: Simulation and test consists of various types and scope of exercises designed to test and evaluate the COOP. In the structured walk-through, a disaster scenario is established, and the teams "walk-through" their assigned tasks. This is role-playing activity that requires the participation of at least the team leaders and their alternates. A tactical exercise is a simulated exercise, conducted in a "war game" format. All members of the continuity organization are required to participate and perform their tasks and procedures under announced or surprise conditions. The exercise monitor provides information throughout the exercise to simulate events following an actual disaster. In a live production system exercise, an operating system is brought to live status on alternate platforms, and the data and communications network is switched to the alternate site. All resources, other than IT and communications hardware and software needed to support the exercise, must be retrieved and deployed from off site (protected) storage, as applicable. A simulation requires the execution of otification, operating procedures, the use of equipment, hardware and software, possible use of alternate site(s), and operations to ensure proper performance. Simulation exercises should be used in conjunction with checklist exercises for identification of required plan modification and staff training.

(a) Announced exercises are scheduled exercises generally involving actual resumption of IT and other critical operations (e.g., command and control) at alternate site(s). IT operations are usually not interrupted but may be planned for actual resumption and validation at the "Hot Site." This type of test usually involves the entire continuity organization, including selected users along with Senior Management, operations and technical staff. Unannounced exercises are surprise exercises that require transfer of operations activity to the alternate site. All required activity continues in parallel and is not interrupted. This type of test generally involves only a small portion of the continuity organization.

(b) To ensure that testing is performed in a cost-effective manner, while still accomplishing the objective of validating the COOP, a separate test plan, with specific scenarios and outlines of acceptable responses, should be developed and followed by management representatives, such as the team conducting the test.

(c) Because the plan will become dated as time passes and resources change, responsibility for maintaining and updating the COOP should be specifically assigned. Maintenance of the COOP can be incorporated into procedures for change management so that upgrades to hardware and software are reflected in the Plan.

CHAPTER 4. Continuity of Operations Planning - Concept of Operations

4.1 Introduction

4.1.1. A Continuity of Operations Plan will be developed to assist an organization in preventing and responding to events that might disrupt mission-essential operations and services, where possible, and to minimize the potential impact of any unavoidable disruption.

a. A Continuity of Operations Plan recognizes the possibility that individuals may execute resumption and recovery operations with limited prior exposure to or knowledge of the entire plan in detail.

b. The Continuity of Operations Plan's development should focus on the following issues:

(1) Heightened awareness of management and employees.

(2) Resumption of essential operations.

(3) Advance preparation to minimize impact potential.

(4) Training in the execution of predefined and preassigned responsibilities and tasks.

(5) Incorporation, when appropriate, of existing contingency plans for IT resources as required under OMB Circular A-130.

4.1.2. The Continuity of Operations Plan will include the strategies, actions, and procedures established to resume mission-essential operations (Requirement 30204).

4.1.3. The Continuity of Operations Plan should also contain a statement of management policy (Requirement 30205). It identifies the plan's objectives, its scope and limitations, the assumptions made during its development, and guidelines for administering the plan's contents (Requirement 30206).

4.1.4. A sample Continuity of Operations Plan format is provided in Appendix C.

4.2 Objectives

4.2.1. To assist the affected organization in resuming mission-critical, time-sensitive business operations and services, its technology, and its support operations in a timely and organized manner in order to continue as a viable and stable entity.

4.2.2. The primary objectives of a Continuity of Operations Plan are to--

a. Provide a tested vehicle which, when executed, will permit and support a safe, efficient, timely resumption of the interrupted essential operation(s).

b. Identify those mission-essential operations that, by nature of their criticality, cannot be disrupted under any circumstance.

c. Ensure the continuity of the essential operations or services provided from the affected facility and organization.

d. Minimize inconvenience and potential disruption to other operations.

e. Minimize the impact to NASA's public image and adverse financial effects of an event.

f. Resume technology operations and communications support for mission-critical and time-sensitive NASA essential operations in the event existing operations have been rendered inoperable.

g. Reduce operational effects of a disaster on NASA mission-critical and/or time-sensitive essential operations through a set of predefined and flexible procedures to be used in directing recovery operations.

h. Resume production processing of the most time-sensitive IT systems, network services, communications, and applications within (e.g., immediate, 8 hours, 24 hours), following the disruptive event.

i. Resume production processing of less time-sensitive IT systems, network services, communications, and applications within (e.g., 5 to 30 calendar

days),following the disruptive event.

j. Resume full operational capability, including test and development work, for technology and operations within (e.g., 30 to 45 calendar days),following the event as permitted by the restoration effort.

k. Resume and maintain adequate service levels to supported organizations.

l. Provide a proper work environment for displaced staff while the facility and its contents is being restored.

m. Ensure that normal operations are restored in a timely manner.

n. Provide the organization with a viable, well-maintained plan.

4.2.3. A Continuity of Operations Plan also seeks to minimize the following:

a. The number and frequency of "ad hoc" decisions that must be made following a disaster.

b. An individual organization's dependence on the participation of any specific person or group of persons.

c. The need to develop and implement new procedures once the disaster has occurred.

d. The loss of vital data and information, recognizing that some loss is inevitable.

e. Confusion and exposure to errors, omissions, and unnecessary duplication of effort.

f. The total elapsed time to execute response, recovery, and restoration processes.

4.3 Scope

4.3.1. The scope of the Continuity of Operations Plan will include mission-essential, time-sensitive, and less time-sensitive operations, supporting IT, and other supporting infrastructure (Requirement 30212).

4.3.2. The Continuity of Operations Plan will be activated in the event that an essential function, or a portion of it, is involved in an emergency, or is declared unable to be performed in its primary location with primary support infrastructure (e.g., staff, data and communications systems, utilities, facility, furniture) (Requirement 30213).

4.3.3. The Continuity of Operations Plan will address resumption and recovery of essential operations, in a disastrous event situation (Requirement 30214). It should not separately address building emergency and evacuation procedures or onsite resumption and recovery procedures, but should incorporate or reference existing emergency-preparedness procedures implemented under other NASA directives.

4.3.4. Actions related to the physical restoration process, in terms of primary site restoration, recovery deactivation, migration and reestablishment of normal operations, termination and shutdown of recovery operations at alternate sites, and postrecovery operations, will be addressed in individual continuity team tasks (Requirement 30215).

4.3.5. The Continuity of Operations Plan will be based on NASA Center management knowledge, review and approval of those mission-critical essential operations, applications, and associated support operations identified as time and/or mission-sensitive (Requirement 30216).

a. The time sensitivity of the essential operations and support activity performed by the organization will be documented during the preplanning process known as a business plan analysis outlined in chapter 3, paragraph 3.3.1 (Requirement 30217).

b. The business plan analysis identifies the time-sensitive, mission-essential operations, IT requirements, time-sensitive support operations, and tolerable outage periods, where appropriate, for which and after which disruptions could result in significant losses to NASA.

c. The resulting application of recovery priorities, on which the Continuity of Operations Plan is based will be documented in a report Essential Processes by Criticality to be included in Continuity of Operations Plan appendices (Requirement 30219).

4.4 Situation

4.4.1. NASA activities take place at different locations, and consequently, potential emergencies may be varied.

4.4.2. Site plans for NASA Centers and details on the types of emergencies that each NASA Center could expect to face are contained in the individual Center Emergency Preparedness Program Plans.

4.5 Assumptions

4.5.1. A NASA mission-essential infrastructure asset (e.g., function, facility(ies), system), or other essential resource(s), are totally unusable or inaccessible, and there is no salvageable equipment, data, or documentation.

4.5.2. The Continuity of Operations Plan is designed for "worse-case" scenarios and depends, to a large degree, on the ability to resume operations from less serious interruptions through the activation of contingency plans established under Agency emergency-preparedness documents or those developed under OMB Circular A-130 for IT resources.

4.5.3. In circumstances involving a localized event (i.e., limited to a single facility and system) equipment vendors and local utility companies should normally be able to install replacement IT and communications hardware and telephone circuits in '1' to '5' calendar days. This assumes that replacement service and equipment orders are placed on an "emergency" basis at the time of the event. It also assumes that the individual NASA Center or facility can quickly obtain and prepare suitable alternate site(s) to serve as an interim temporary resumption and recovery activity for its business operations and information processing centers, in a period of 3 to 5 days.

4.5.4. In the event of a regional emergency, such as an earthquake or a tornado, it could take weeks to acquire the necessary equipment and data circuits. This will be due to multiple organizations contending for the same emergency resources and services. Regional emergencies which cause wide-spread disruption of public utilities such as electricity, water, and network services may also cause additional delays in reestablishing NASA business and technology operations without preidentified, preconditioned, and contractual alternate backup sites.

4.5.5. That NASA Centers and organizations will have access to and use of sufficient physical sites within the NASA environment to meet its resumption and recovery time objectives. Sites currently considered eligible temporary recovery locations are listed in the individual Continuity of Operations Plan as an appendix. The repositioning of redundant equipment and operational capability, environmental conditioning, and access to the NASA WAN which may be necessary to accomplish recovery actions is also addressed in the Continuity of Operations Plan as an appendix.

4.5.6. Level of documentation in the individual Continuity of Operations Plan assumes and requires that NASA management and staff are familiar with the Center's or organization's business operations, its supporting resources configuration, and the requirements of the Continuity of Operations Plan.

4.5.7. Sufficient management and staff, familiar with and trained in the procedures and tasks in the individual Continuity of Operations Plan, will be available subsequent to the interrupting event to execute their recovery responsibilities and to support the restoration effort. NASA personnel understand that, following a major interruption of essential operations, it will not be a matter of "business as usual" but "survival."

4.5.8. All vital business documentation and files necessary for resumption and recovery purposes are backed up and stored and located safely away from the critical facility(ies) using a rotation schedule that minimizes the data loss.

4.5.9. All vital electronic data files required to implement resumption of the current operating environments, and/or that support time-sensitive essential operations are backed up daily.

a. When appropriate, this information is rotated to a safe offsite location according to a schedule that minimizes data loss and the effort to reconstruct production environments.

b. The type of backups and the timing of the offsite rotation and retention are approved by NASA management and are considered sufficient to minimize the reentry and reconstruction of data and the re-creation, forward recovery of files to current status.

4.5.10. All vital backup items for resumption and recovery are stored onsite and offsite or can be easily and quickly obtained or created from other identified sources.

a. The backups stored onsite are in a series of fire resistant safes that are located within the Center and organization boundaries.

b. The backups stored offsite are in a secured location that is sufficiently distant from the primary site so they would be unaffected by most interrupting events.

c. These stored backups are considered to be the only resources available to implement resumption.

d. The Continuity of Operations Plan assumes that locations where backups are stored were not affected by the emergency incident or situation and can be accessed by NASA personnel.

4.5.11. All information necessary to complete the internal and external contacts quickly and accurately during resumption is documented and maintained in the Continuity of Operations Plan.

4.5.12. The timeframe in which each time-sensitive essential function, supporting activity, and IT system has been set is current with the needs of clients and is available within the Continuity of Operations Plan.

a. The resumption of each essential function is greatly dependent on the availability of appropriate staff, its information, communications, and its access to the IT systems and data files, if required.

b. Actual timeframes for resumption and recovery may be influenced by the availability of staff, alternate operating sites, hardware and software, current backup files, and the reload time requirements of the IT system architectures.

4.6 Recovery Strategy

4.6.1. Loss of functionality of essential operations (e.g., facilities, systems, other interdependencies) at a NASA location may have a significant impact on data delivery at the Center and organizational level, and in some instances, throughout NASA.

4.6.2. The Continuity of Operations Plan will be developed to respond effectively to a significant event by using a predefined method for utilizing various facility, staff, and technical resources (Requirement 30238). This method, known as the recovery strategy, is employed to help ensure that an affected organization can accomplish the resumption and recovery of mission-essential operations within stated timeframes at required levels of service.

4.6.3. Consideration must be given to selecting a recovery strategy that is workable as well as cost efficient (Requirement 30239).

4.6.4. A COOP recovery strategy should anticipate the availability of other NASA and Federal agency locations for use as alternate operation sites. (A prioritized list of eligible locations should be provided as an appendix to the Continuity of Operations Plan.)

4.6.5. Alternate sites should be selected for their ability to support physical and technical infrastructure requirements while providing the best possible access to essential communications resources (e.g., telephones, WAN/LAN), as necessary to meet essential requirements (Requirement 30241).

4.6.6. As appropriate, the Continuity of Operations Plan will ensure planning for continuity teams including relocating to selected alternate sites and preparing

them for use as alternate operating sites should an event require activation of the Continuity of Operations Plan (Requirement 30242).

4.6.7. Where the Continuity of Operations Plan provides for prepositioned equipment and services, COOP teams will activate those resources as necessary (Requirement 30243).

4.6.8. Where additional equipment and other services are needed to upgrade a site to full utilization, these items will be acquired and installed on an emergency basis (Requirement 30244).

4.6.9. Configuration details for current servers, and network management devices are included in the Continuity of Operations Plan to help expedite this "acquire time of disaster" strategy as are the current inventory of NASA contracts for which emergency requisitions will be drafted (included in the Continuity of Operations Plan appendices) (Requirement 30245).

4.7 Plan Administration

4.7.1. The scope of administrative duties and responsibilities includes, but is not limited to, the continued endorsement of the Continuity of Operations Plan by affected program management, through mandatory, documented review of the Continuity of Operations Plan by appropriate management personnel and team members, on no less than an annual basis (Requirement 30247).

4.7.2. A report on the plan's administration, prepared by the responsible program or project management, will be reviewed and approved by the Agency Senior Management official responsible for the COOP program, annually or as otherwise required (Requirement 30248).

4.7.3. The affected Program Manager, or his/her designee, is responsible for administration of the plan (Requirement 30249).

a. He/she will ensure that NASA standards and procedures are developed to address COOP administrative needs (Requirement 30250).

b. He/she will also include any relevant, related documentation in the plan (Require (Requirement 30251).

c. As custodian and administrator of the Continuity of Operations Plan, he/she must have a thorough knowledge of all plan contents (Requirement 30252).

d. As a further safeguard, he/she should never be the sole person in the organization with extensive knowledge of the structure and contents of the plan (Re

(Requirement 30253). An alternate COOP coordinator will be a full participant in all plan maintenance and exercise activities (Requirement 30254).

4.7.4. Responsibility for maintaining specific sections of the Continuity of Operations Plan resides with each COOP Team Leader in accordance with the Team's objectives and functional responsibilities for Prevention, Response, Resumption, Recovery, and Restoration (Requirement 30255).

a. Team leaders must ensure compliance with these documented procedures for plan administration (Requirement 30256).

b. Each employee, regardless of their role as a COOP team member, is responsible for providing updated personal contact information to the responsible Program or Project Manager, as changes occur (Requirement 30257).

4.7.5. Each employee is responsible for the maintenance of the affected organization's capability to respond and resume essential operations following a disaster. (Requirement 30258).

a. Some individuals will have more direct responsibility than others will.

b. Each individual must be aware of the necessity for the preservation of such a continuity capability and must ensure that the Prevention, Response, Resumption, Recovery, or Restoration capability is truly viable (Requirement 30260).

c. Should a plan review necessitate changes or updates, the COOP Coordinator is responsible for implementing the changes and issuing updated plan documentation(Requirement 30261).

d. Individuals in responsible management positions will be called upon periodically to provide information necessary for maintaining a viable plan and an exercised continuity capability (Requirement 30262).

4.8 Continuity Process Overview

4.8.1. This section outlines the four major stages of the continuity process as it applies to development and maintenance of a Continuity of Operations Plan.

4.8.2. It describes the central activities and objectives of each stage and the relationships between stages.

4.8.3. Actual circumstances of the business interruption disaster will determine whether a particular stage is initiated and how long it will take to complete.

4.8.4. This section provides guidelines and explains the continuity process.

4.8.5. Emergency Response

Following the notification of the emergency incident or situation, and in accordance with Agency and individual Center Emergency Preparedness Response Plans, a team of key COOP personnel, the COOP Assessment team, will first assemble at the incident site, or other staging area if the incident site is deemed unsafe, contaminated, or otherwise unsuitable for use, and begin to assess and evaluate the site(Requirement 30268).

a. Primary objectives of the COOP Assessment Team are--

(1) To operate safely and efficiently.

(2) To establish an immediate and controlled presence at the incident site, as allowable per instructions of the onscene incident commander in accordance with Center Emergency Preparedness Response Plans.

(3) To conduct an onsite (and in some instances "standoff") assessment of the incident impact, known injuries, extent of damage, and disruption to the facility(ies), services, and business operations.

(4) To determine if and/or when access to the facility(ies) will be allowed.

(5) To provide the appropriate management team with the facts necessary to make informal decisions regarding subsequent recovery activity.

b. Response to an emergency does not necessarily or automatically translate into the declaration of a disaster and the implementation of a COOP.

c. Activation of the disaster recovery portion of the Continuity of Operations Plan requires significant expenditures of time, personnel, and financial resources. The appropriate affected program management team will determine whether or not the expenditure of resources are warranted and to what extent they are justified, based on the information and recommendations provided by the Assessment Team (Requirement 30271).

4.8.6. The appendices of the Continuity of Operations Plan will contain up-to-date contact lists, team assignments, checklists of specific tasks to be performed, and copies of any individual contingency plans developed under OMB Circular A-130 (Requirement 30272). The flowchart below (Figure 3) provides a graphical overview of the NASA COOP Emergency Response Process.

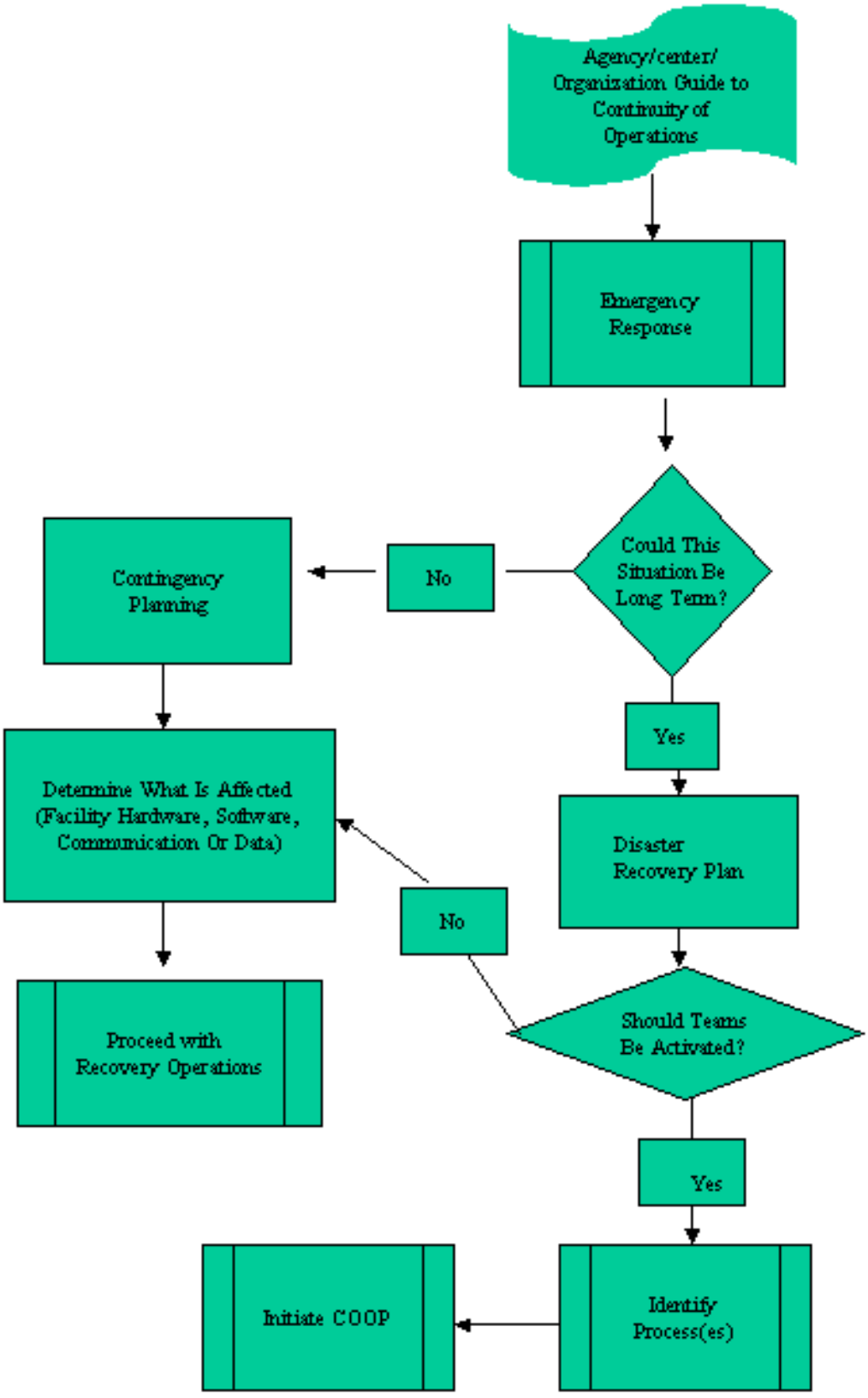

Figure 3: COOP Emergency Response Process

4.9 Incident Alert

4.9.1. Initial notification of an incident or situation is generally expected to come directly from an affected organization staff member or the discoverer of the event. Other potential sources of incident notification might be law enforcement, security, fire department, other Center emergency response personnel, and news media.

4.9.2. The Continuity of Operations Plan will provide instructions for the proper and timely notification of an emergency situation, including notification to Center management, Center Emergency Response management personnel, and appropriate Headquarters personnel per requirements of NPD 8710.1, Emergency Preparedness Program, and NPR 8715.2, NASA Emergency Preparedness Plan Procedural Requirements (Requirement 30275).

4.9.3. The Continuity of Operations Plan will provide specific instructions and guidelines for contacting members of the continuity management team and the various response teams (Requirement 30276). Notification procedures will also include requirements for maintaining records of all notifications made (Requirement 30277).

4.9.4. Notification Guidelines

The individual Continuity of Operations Plan will include instructions and guidance for the following:

a. All team leaders and team members should be assigned call tree responsibilities that will be followed during the emergency notification (Requirement 30279). The appropriate Center Director will determine if the facility should be declared a disaster, based on a preliminary assessment of the situation (Requirement 30280).

b. If emergency notification procedures are initiated, each team leader will be responsible for contacting their alternate team leader and team members with specific instructions (Requirement 30281).

c. If the team leader is not available, the alternate team leader will assume the team leader's responsibilities (Requirement 30282).

d. In the event the alternate team leader is also not available, the management team will assign someone to complete the notifications until the primary or alternate team leaders become available and resume their responsibilities (Requiren (Requirement 30283). It is important that all key personnel be notified of the disaster as soon as possible to begin resumption of essential operations.

e. An Employee and Contractor Notification List will be developed and maintained that has the telephone numbers of essential personnel to be notified in a predetermined sequence (Requirement 30284).

4.9.5. Objectives of the Continuity Organization During Emergency Response

The objectives for the continuity organization during emergency response are as follows:

a. Complete emergency response, notification, and mobilization duties as directed by the COOP Management Team.

b. Ensure that the COOP Management Team is contacted and apprised of the emergency situation's status and activity.

c. Obtain situation reports of personnel injury, damage, and other related matters from Center Emergency Response management personnel.

d. When permitted to do so by Center Emergency Response authorities, perform assessment(s) and evaluation(s) until the extent of impact or damage can be reasonably determined.

e. Document the results of preliminary assessment(s) and evaluation(s) and submit the report to the COOP Management Team with recommendations to terminate the emergency response activities or activate subsequent plan operations.

f. Terminate, expand, or extend the operation as directed by the COOP Management Team.

4.10 Resumption

COOP planners will ensure that the organization's Continuity of Operations Plan contains specific guidance for the following activities:

4.10.1. Establishing and organizing a Command Center from which to manage resumption activities (Requirement 30287).

a. This Command Center may be collocated with the Center Emergency Operations Center (EOC) if activated by Center Management.

b. If the disastrous event is of a scale that impacts the entire Center, multiple COOP activity may be implemented.

c. Refer to the Center Emergency Preparedness and Response Plan for guidance.

4.10.2. Activating and mobilizing the continuity teams needed to resume time-sensitive restoration activity (Requirement 30288).

4.10.3. Evaluating alternate site equipment and network service for the necessary enhancement to support time-sensitive application recovery (Requirement 30289).

4.10.4. Mobilizing and activating the support teams needed to support enhancement and use of the alternate site(s) (Requirement 30290).

4.10.5. Notifying and informing clients and NASA Senior Management of the situation (Requirement 30291).

4.10.6. Alerting employees and contractors not assigned to the continuity organization, vendors, and other key organizations to the situation and their role, if any, during resumption and recovery (Requirement 30292).

4.10.7. Once mobilized, the support teams will be instructed in their reporting and action requirements (Requirement 30293). The necessary site assessments, evaluations, and the initiation of salvage operations will be completed once the Command Center is established (Requirement 30294). Additional alerts to supporting vendors, management, and customers will also be conducted from the Command Center (Requirement 30295).

4.10.8. Based on the information and recommendations provided by the Assessment and Salvage Team, the COOP Management Team will determine whether or not the expenditure of resources are warranted, to what extent they are justified, and what other actions will be taken (Requirement 30296).

4.10.9. Objectives of the resumption stage

The objectives that will become the major focus of the resumption stage are--

a. To prepare for and/or implement the procedures necessary to facilitate and support the resumption process and subsequent restoration operations, as required.

b. To mobilize and activate the continuity teams responsible for reestablishing essential operations and functions.

c. To alert employees, vendors and other internal and external individuals, and organizations.

d. To begin implementing procedures to restore and establish time-sensitive

processes and applications. This may include relocating to a temporary facility, reestablishing communications at an alternate site, or activation of a redundant site.

4.11 Command Center

4.11.1. A Command Center will be established if management decides to continue and escalate the situation from emergency response to resumption operations. The site for the Command Center should be identified in advance. Initial activities performed at the Command Center are described below.

a. If the facility can be accessed, further assessments and evaluations of the onsite conditions, the damage impact and extent of the emergency incident or situation will be completed.

b. Use of the command center may be confined to management meetings and the cancellation of resumption operations if the facility (e.g., work areas, fixed assets, files, equipment, voice communications) are unaffected and the emergency incident or situation problems can be resolved without major impact to the critical operations.

c. If the information about the emergency incident or situation problems is inconclusive, the Command Center will be used as a meeting site until the assessments are completed.

d. If the emergency incident or situation is such that the resumption operation needs to be continued or further escalated, and/or a disaster declared, the Command Center should be organized and the appropriate support and resumption teams notified and activated as required.

4.12 Recovery

4.12.1. The recovery stage of the continuity process concerns the reactivation of a greater scope of operations and services beyond the most time-sensitive operations.

a. Management, through development and implementation of the COOP will initiate recovery-stage operations if the estimate of total outage indicate the need to expand service delivery using alternative locations and resources.

b. If, for example, the impact on the facility is expected to take more than 30 days to resolve, the recovery stage may be initiated at alternative site(s) and the

appropriate resources devoted to those applications.

c. Alternatively, if it is estimated that 15 days would be needed to restore to full operations, organization management might initiate a parallel effort to resume less time-sensitive operations at another site while planning the migration of resumption activities from the alternate site(s) to the primary facility.

d. Consequently, recovery, resumption, and restoration stage activities may be conducted with some parallelism as dictated by the situation.

4.12.2. Objectives of the recovery stage

The objectives for recovery stage operations include--

a. Maintaining a Command Center, which provides sufficient direction and support for resumption and recovery operations.

b. Mobilizing and activating additional continuity teams to facilitate the recovery of less time-sensitive operations.

c. Maintaining an adequate level of support team coverage to support all operations.

d. Maintaining an adequate level of technology team coverage to sustain information processing service demands as they grow in scope.

e. Maintaining communication with the continuity organization, clients, and Senior Management.

4.12.3. Command Center During the Recovery Stage

The level of support maintained at the Command Center during recovery will be determined by the Management Team based upon--

a. Scope of the disaster,

b. Number of essential operations affected,

c. Level of support required for the recovery of essential operations, and

d. Perception of ongoing risks and/or exposures.

4.13 Restoration

4.13.1. When Center Emergency Response officials allow access to the facility, the COOP Management Team will initiate the restoration phase of the COOP.

4.13.2. The restoration stage builds on the assessments performed in the emergency response stage with the goal of returning the impacted facility to its predisaster capabilities. In circumstances where the original facility was assessed as beyond repair, this stage will involve the acquisition and outfitting of new permanent facilities.

4.13.3. The Restoration process will include the assessment of--

a. Environmental contamination of the affected areas,

b. Structural integrity of the building, and

c. Damage to furniture, fixtures, and equipment.

4.13.4. Restoration will begin when reliable estimates of contamination, structural damage, and asset loss can be obtained and personnel resources can be dedicated to the management and coordination of the process. This phase may be executed sequential to, or concurrent with, the resumption and/or recovery stages.

4.13.5. Objectives of the Restoration Stage

In addition to maintaining a Command Center that provides sufficient support for resumption and restoration operations, objectives of the restoration stage are to--

a. Maintain an adequate level of support team coverage to support all operations,

b. Maintain an adequate technology teams coverage to sustain information processing operations, when required,

c. Maintain communication with the continuity organization,

d. Clean and/or decontaminate the facility,

e. Repair and/or restore the facility or construct or acquire a new facility,

f. Replace the contents of the facility, and

g. Coordinate the relocation and/or migration of business operations (e.g., personnel, equipment) from temporary facilities to the repaired or new facility.

4.14 Continuity Team Organization

4.14.1. In the event of a disaster, the normal structure of the unit must shift to that of the continuity organization.

4.14.2. The affected organization will shift from the current "business as usual," structure to an organization working towards survival and the resumption of time-sensitive essential operations.

4.14.3. The teams associated with the COOP represent units and/or support operations organized to respond, resume, recover, or restore essential operations of the affected facility. See Figure 2, chapter 3, for a representative organizational chart of a typical continuity team.

4.14.5. Each team is comprised of individuals with specific responsibilities or tasks that must be completed to fully execute the COOP.

4.14.6. A primary and alternate team leader who is responsible to the affected Program Manager, or his/her designee, leads each team.

4.14.7. Each team is a subunit of the continuity organization.

4.14.8. Each team is structured to provide dedicated, focused support, in the areas of its particular experience and expertise, for specific response, resumption, and recovery tasks, responsibilities, and objectives.

4.14.9. A high degree of interaction among all teams will be required to execute the COOP.

4.14.10. Each team's eventual goal is the resumption and recovery and the return to stable and normal business operations and technology environments.

4.14.11. Each team leader will report status and progress updates to its management team throughout the continuity process.

4.14.12. Close coordination must be maintained with the appropriate management personnel and each of the other teams throughout the resumption and recovery operations.

4.14.13. The primary responsibilities of the continuity organizations are to--

a. Protect employees and information assets until normal business operations are resumed.

b. Ensure that a viable capability exists to respond to an incident.

c. Manage all response, resumption, recovery, and restoration activities.

d. Support and communicate with NASA Senior Management and other locations, as necessary.

e. Accomplish rapid and efficient resumption of time-sensitive business operations.

f. Ensure that all statutory and regulatory requirements are satisfied (e.g., environmental, records retention).

g. Exercise impact resumption and recovery expenditure decisions.

h. Streamline the reporting of resumption and recovery progress among the teams and with the affected program management team and NASA Senior Management.

4.14.14. During Emergency Response, the primary responsibilities of the continuity organizations are to--

a. Establish an immediate and controlled presence at or near the incident site and await instructions from Center emergency response personnel.

b. Determine if and/or when access to the facility will be allowed.

c. Upon being granted permission to enter impacted facility, conduct a preliminary assessment of incident impact, extent of damage, disruption to the affected organization's services and essential operations.

d. Provide Center Senior Management with the facts necessary to make informed decisions regarding subsequent resumption and recovery activity.

4.14.15. During Resumption, the primary responsibilities of the continuity organization are to--

a. Establish and organize a Command Center for the resumption operations.

b. Notify and apprise team leaders of the situation.

c. Mobilize and activate the operations teams necessary to facilitate the resumption process.

d. Alert employees, vendors, and other internal and external individuals and organizations.

4.14.16. During recovery, the primary responsibilities of the continuity organization are to--

a. Prepare for and/or implement procedures to facilitate and support the recovery of less time-sensitive operations.

b. Mobilize additional continuity teams and support organizations as required.

c. Maintain an information flow regarding the status of recovery operations among employees, vendors, and other internal and external individuals, and organizations.

4.14.17. During Restoration, the primary responsibilities of the continuity organization are to--

a. Manage salvage, repair and/or refurbishment efforts at the affected facility.

b. Prepare procedures necessary for the relocation or migration of operations to a new or repaired facility.

c. Implement procedures necessary to mobilize operations, support, and technology relocation or migration.

d. Manage the relocation/migration effort as well as perform employee, vendor, and customer notification before, during, and after relocation or migration.

4.15 Plan Activation

4.15.1. Activation of the COOP should only be executed when an emergency occurs that necessitates a response beyond the scope of daily standard operating procedures. In accordance with Agency and/or individual Center Emergency Preparedness Program Plans, only the following selected personnel may activate the entire plan, or any phase thereof, and/or declare a disaster situation for NASA.

a. The NASA Administrator or designee may declare a NASA emergency.

b. The Center Director or his/her designee will decide whether or not to activate the respective organizational COOP and/or declare a disaster.

4.15.2. Their decision will be based on a preliminary assessment of the business interruption incident, including any physical impairment to the facility. Pending their decision, emergency notification of NASA personnel will be initiated, and the entire COOP, or any phase thereof, will be activated, as directed.

4.15.3. Technology teams focused on restoring communications, data, networks, will be activated only as directed by the management team. Each team consists of unique procedures, tasks, contact, and resource information. Programs and applications will be restored according to established priorities.

4.15.4. Organization restoration teams will be activated only as directed by the

Management Team based on the impact of the disruption. Restoration priorities will be established in response to the disruption. Staff will focus on reestablishing essential office operations and ensuring that the restoration teams focus on communications, application, and program recovery priorities.

4.16 Team Roles and Responsibilities

4.16.1. Following the response phase of the COOP, the affected organization will organize into teams to execute its resumption and recovery activities on behalf of NASA.

4.16.2. To accomplish the tasks assigned, each team will draw upon the expertise of supporting organizations, both internal and external, as necessary.

4.16.3. This section of the COOP will identify the major groups of teams required to accomplish recovery.

4.16.4. Each team has a minimum of a leader and one or more members representing the skills appropriate to the team's role.

4.16.5. Team leaders/alternates must be thoroughly familiar with the responsibilities not only of their team but also of all the teams with which they must interact.

4.16.6. A detailed list of teams and their current team members will be located in the Plan Implementation section of the COOP.

4.16.7. The roles and responsibilities of each major group of teams are outlined below.

a. Affected Program Management

(1) Approve the activation of the plan or the declaration of a disaster.

(2) Approve expenditures as required.

(3) Coordinate temporary relocation logistics with support services organizations.

(4) Coordinate with NASA Senior Management on the issuance of related news releases to the press and media.

(5) Monitor all activities with the Recovery and Restoration Management Teams.

(6) Provide Senior Management direction and counsel to activated teams as required.

(7) Coordinate all personnel matters and issues involving employee fatalities and injuries and notifications to employee's families and dependents with NASA management. This may also include professional counseling and financial support for employees.

(8) Review progress and status with Center and NASA Senior Management.

(9) Manage the resumption and recovery of all business operations and service delivery.

(10) Establish and organize a business resumption operation at an alternate site.

(11) Organize the business resumption Command Center.

(12) Direct and support team leaders and make assignments, as appropriate.

(13) Ensure that a damage assessment and salvage operation is conducted at the primary site.

(14) Control the activation of the business resumption procedures.

(15) Coordinate the eventual restoration and relocation of the primary site.

(16) Report resumption and recovery progress to NASA Senior Management.

b. IT Resources, Communications and Data Recovery Management

(1) Contact key personnel required for resumption of time-sensitive operations.

(2) Alert all personnel and instruct them to report to their designated areas, as required.

(3) Perform tasks to resume time-sensitive operations, as required.

(4) Work with support teams to obtain support required for task accomplishment.

(5) Report the status of resumption activity to management team.

(6) Manage all administrative activities associated with the resumption and recovery operations.

(7) Notify alternate backup sites and/or vendors of disaster declaration. Ensure that backup sites are prepared to accept staff for resumption of operations.

(8) Identify and coordinate procurement actions for equipment and services for alternate site installation, if not a redundant site.

(9) Identify and retrieve all backup files and other vital records from offsite or remote storage.

(10) Request and coordinate installation of data and telecommunications capability if necessary.

(11) Execute IT systems resumption procedures.

(12) Manage IT systems operations at the alternate and primary sites if necessary.

c. Organization Restoration Management

(1) Coordinate salvage and/or reconstruction of the affected facility, records, and file reports, as appropriate.

(2) Coordinate the acquisition and outfitting of a new permanent site, if necessary.

(3) Identify and coordinate procurement for equipment and services for the permanent site.

(4) Work with NASA support teams to obtain required services to restore and outfit a permanent office location.

(5) Manage preparation of a migration plan from the alternate site to the permanent site.

(6) Coordinate migration and move-in logistics with the affected management, IT Communications and Data Recovery teams, and with NASA support services.

4.17 Reporting Structure

The Program Manager, or his/her designee, will develop a reporting structure for the continuity organization that reflects the overall team organization and reporting requirements that will be employed during response, resumption, recovery, and restoration processes.

4.18 Plan Maintenance

4.18.1. COOP maintenance procedures are divided into two general categories, scheduled and unscheduled. Scheduled plan maintenance is time-driven, where unscheduled plan maintenance is event driven.

4.18.2. Scheduled Plan Maintenance

a. Scheduled maintenance may consist of quarterly reviews and updates as well as annual structured walk-through and/or tactical exercises (as described in the Plan Exercise section of this document).

b. The purpose of the COOP review is to determine whether changes are required to the procedures, the continuity organization, and notification procedures.

c. The Program Manager, or his/her designee, is responsible for initiating scheduled maintenance activities in consultation with the Management Team.

d. The Program Manager, or his/her designee, shall initiate semiannual continuity plan reviews. He or she shall notify all continuity organization team leaders and alternate team leaders to review the response, resumption, recovery, and restoration task lists, contact information and procedures for changes that may be required.

e. Other organization staff members may be invited to satisfy the needs of a specific review session.

f. The reviews address events that have occurred within each team's area of responsibility that may affect the response, resumption, recovery, and restoration capability.

g. Teams shall submit changes to the Program Manager, or his/her designee, as they are needed. The Program Manager, or his/her designee, shall incorporate all changes to the COOP and distribute updated copies, as required.

4.18.3. Unscheduled Plan Maintenance

a. Certain maintenance requirements are unpredictable. The majority of unscheduled changes occur as the result of major changes to service level agreements, hardware configurations, networks, and production processing.

b. Examples of items that may trigger the need for unscheduled maintenance of the plan may include:

(1) Changes in data processing architectures, hardware, or environmental changes.

(2) Major changes in operating system(s) or utility software programs.

(3) Major changes in the design of a production database.

(4) Major changes in communications, systems network design, or

implementation.

(5) Changes in offsite storage facilities and methods of cycling items.

(6) Improvements or physical changes to the current facility.

(7) Changes in the business or operating environment.

(8) Center and/or Enterprise organization changes that affect continuity teams.

(9) New application systems development.

(10) Discontinuation of an application systems from processing schedules.

(11) Transfers, promotions, or resignations of individuals on the emergency notification list or continuity organization teams.

(12) Significant modification of basic operations, data flow requirements, or accounting requirements within an application system.

c. The Program Manager, or his/her designee, must be made aware, in writing, of all changes to the COOP resulting from unscheduled maintenance.

d. The Program Manager, or his/her designee, shall then notify all continuity organization team leaders and alternate team leaders to review the COOP for changes that will be required as a result of the item that has triggered the review.

e. Team leaders will submit actual change data to the COOP Coordinator.

f. The Program Manager, or his/her designee, will team up with the person submitting the change and either update the COOP or assign the update responsibility to the affected continuity team(s). Cross-team coordination should be completed within 2 weeks of the review.

g. The Program Manager, or his/her designee, is responsible for any required updates to the Plan, which result from the review.

h. The Program Manager, or his/her designee, shall print hard copies of the Plan, and distribute as required.

4.19 Resumption and Recovery Configuration

4.19.1. The Continuity Plan maintenance process should include a periodic re-evaluation of the minimum staffing, technical support, and services required to provide short-term response, resumption, recovery, and restoration capability.

4.19.2. When IT support is integral to the continuation of essential operations, the reevaluation process must also address the capacity growth requirements associated with the increase of transaction processing volumes of the production application systems, as well as the addition of new systems to the production environment.

a. Based on the existing configuration and requirements, it is assumed that the most effective configuration for supporting long-term recovery and restoration will be the installation of the computer hardware required to support normal to near-normal levels of processing in a temporary environment.

b. Special attention is required to ensure continuing compatibility of existing equipment with that which is installed at the alternate site.

4.20 Plan Exercises or Tests

4.20.1. Documentation and periodic reviews of the organization COOP are useful. However, proof and confidence that the COOP will work only results from completion of a successful exercise or test of the tactical strategies and procedures. Exercises and tests of the individual organization and system COOP are designed to determine--

a. The state of readiness of the continuity organization to respond to and cope with a disaster involving mission-essential operations, facilities, and IT systems and other interdependencies,

b. Whether backed up vital data and records stored offsite are adequate to support resumption of essential operations,

c. Whether inventories, tasks, and procedures are adequate to support resumption of essential operations, and

d. Whether the organization COOP has been properly maintained and updated to reflect the actual resumption, recovery, and restoration needs.

4.20.2. Type and Scope of Exercises or Tests

a. A comprehensive program of exercises and tests varying in scope and level of detail will assist organizations in ensuring the effectiveness of their COOP.

b. Examples of the types of exercises and tests that may be incorporated into the organization training/exercise program are outlined below.

c. At a minimum, organizations having responsibility for COOP activity will test

and document the COOP at least annually, using one or more of the suggested exercise types:

(1) Structured Walk-Through

(a) In the structured walk-through, a disaster scenario is established, and COOP Teams "walk through" their assigned tasks.

(b) This is a "role-playing" activity that requires the participation of at least the team leaders and their alternates.

(c) The developed scenario will be made available in advance of the exercise to allow team members to review their assigned tasks in response to the exercise scenario.

(d) During the structured walk-through, the COOP is checked for any errors or omissions.

(e) At the end of the structured walk-through, any changes to the COOP that are found to be necessary are implemented.

(f) This type of exercise can be conducted with or without an independent "monitor."

(2) Tactical

(a) A tactical exercise is a simulated exercise, conducted in a "war game" format.

(b) All members of the individual continuity team are required to participate and perform their tasks and procedures under announced or surprise conditions.

(c) Participants include an exercise monitor or monitors, depending on the size of the organization.

(d) The exercise monitor(s) provides information throughout the exercise to simulate events following an actual disaster.

(e) Generally, a disaster scenario is established and is provided to all business operations continuity team leaders, alternate team leaders, and team members located in a large conference room, auditorium, or using video teleconferencing.

(f) Each team executes its exercise objectives and interacts with other teams as they complete their actions.

(g) A "speeded up" clock is usually employed in order to complete, at a minimum, 3 days' actions in 1-working day and requires the teams to respond to

the scenario information in near "real" time.

(h) An 8-hour exercise will usually simulate 48 to 72 hours of resumption activity.

(i) As in the structured walk-through, the plan is checked for any errors or omissions.

(j) At the end of the tactical exercise, any changes to the plan that are found to be necessary are implemented.

(3) Live Production

(a) In a live production application systems exercise, an operating system is brought to live status on the alternate processing activity, and the data communications network is switched to the alternate site.

(b) All resources, other than the operating platform and communications hardware needed to support this exercise, must be retrieved from the offsite storage facility, unless an alternate or redundant site is in existence.

(c) This exercise continues to validate the switching capability of the data communications network, and then to the production of selected applications systems, including User Login and application system data currency checks.

(d) A live production exercise will normally be conducted on a weekend when there is a lesser requirement to provide continued service to the user community.

(e) Assurance of overall recoverability can only be achieved through the conduct of a complete Live Production Application System Exercise.

(4) Simulation

(a) This type of exercise requires the execution of notification, operating procedures, the use of equipment hardware and software, possible use of alternate site(s), and operations to ensure proper performance.

(b) Simulation exercises can and may be used in conjunction with "checklist" exercises for identification of required COOP modification and staff training.

(c) Examples of procedures verified during a simulation exercise include emergency procedures, use of alternate methods, telecommunications backups, agent, vendor, customer notifications, hardware capacity and performance, software transportability, alternate site(s) access, team mobilization, offsite file,

information retrieval and input data retrieval.

(5) Announced and Unannounced

(a) Announced exercises are scheduled exercises generally involving actual resumption of overall operational capacity including IT resources.

(b) Production processing is usually not interrupted, but may be planned for actual resumption and validation at the "Hot Site."

(c) This type of test usually involves the entire continuity organization, including selected users along with operations and technical staff.

(d) Unannounced exercises are surprise technical exercises that require processing to be actually recovered at the alternate site.

(e) Production processing continues in parallel and is not interrupted.

(f) This type of test generally involves only a small portion of the continuity organization and few, if any, users.

(6) When to Exercise or Test

d. Exercises or Tests will be conducted when--

(1) The COOP is first developed and implemented,

(2) A major revision to the COOP has been completed,

(3) When significant changes in operating systems, applications and/or data communications has occurred,

(4) The preparedness level of continuity teams must be verified, and

(5) At least annually.

e. Responsibility for Establishing Exercise Scenarios

(1) The Program Manager, or his/her designee, operating under COOP, is responsible for developing the strategy for each exercise.

(2) Development of procedures that measure the effectiveness of the COOP will address the following plan elements:

i. Notification

ii. Organization

iii. Resources and Vital Records

iv. Operations

f. Exercise and Test Scenarios

(1) Exercise scenarios are normally developed to accomplish the objectives established by Senior Management.

(2) Some considerations in developing exercise scenarios include:

i. Reexercising the plan segments that were determined to be deficient in past exercises.

ii. Exercising time-sensitive application systems that have never been recovered or restored, or have not been recently exercised.

iii. Involving those continuity organization team members that need more training and preparation to maintain familiarity with their operations.

iv. Ensuring that each exercise involves the use of only offsite storage and inventory items to ensure completeness and accuracy of the offsite inventory.

v. Deciding whether the exercise and associated parameters will be openly announced or will be a surprise. This decision is usually made at the discretion of the enterprise business continuity officials.

g. Exercise and Test Evaluation

(1) An unbiased evaluation team should be assigned and will evaluate the results of each exercise or test.

(2) This team should be made up of personnel external to the organization conducting the exercise or test.

(3) The evaluation team must be focused entirely on the validity, currency, and capability of the COOP to recover and restore NASA time-sensitive application systems at the alternate site(s).

(4) Recommended members of the evaluation team include --

i. Center Emergency Preparedness and Response Personnel.

ii. Center Safety Officials.

iii. Security Officer.

iv. Vital Records Manager.

v. Program Management.

vi. Other Center Officials, as appropriate.

(5) The Exercise Evaluation Team is charged with the following responsibilities--

i. Familiarization with the overall COOP.

ii. Understanding thoroughly the objectives of the exercise or test to be conducted.

iii. Monitoring and observing all the activities of the teams involved in the exercise or test.

iv. Ensuring that the exercise or test objectives are met, from the organization's and client's perspective.

v. Documenting findings relating to the strengths and weaknesses observed during the exercise or test.

h. Reviewing Exercise and Test Results

(1) Team leaders and program management will document exercise or test results as soon as possible, but not later than 2 weeks after completion of an announced or unannounced exercise or test.

(2) Selected members of the continuity organization will review the exercise and test results and resolve weaknesses and problems.

(3) The project manager, or his/her designee, will chair the review and coordinate appropriate changes and updates to the COOP.

(4) The results of the review will be presented to the Center Director, appropriate management personnel, and the appropriate Enterprise Business Continuity Official(s).

(5) A copy of the exercise or test results will be provided to the Agency and Center COOP coordinators, respectively.

i. Schedule of Exercises

(1) The Program Manager, or his/her designee, will schedule exercises in coordination with the Center COOP Coordinator.

(2) Exercises should be scheduled with consideration to seasonal production and business cycles, the number of processing systems or platforms in production, and the time required to exercise both time-sensitive processes to full production systems.

j. Education and Training

(1) Awareness of the need for and the processing of maintaining a viable continuity capability are essential and federally mandated.

(2) This awareness will be achieved through formal education and training sessions conducted on at least an annual basis.

(3) This provides a way of ensuring that the necessary understanding of the COOP program and processes are understood by the personnel responsible for maintaining and implementing the plan.

(4) The objectives of COOP training are to--

i. Train all key employees and management who are required to help maintain the plan in a constant state of readiness.

ii. Train key employees and management who are required to execute various plan segments in the event of an extended disruption in normal operations.

iii. Heighten planning awareness for those employees not directly involved in maintaining and/or executing the Plan.

(5) The individual Center COOP Coordinator will schedule educational seminars addressing individual COOP activity at least, but not less than, semiannually.

(6) These seminars will include overviews of the--

i. Continuity strategy, priorities, and timeframes.

ii. Business continuity organization structure and responsibilities.

iii. Individual COOP structure and contents.

iv. Data preservation methodologies and practices.

v. Mobilization, transportation, transfer of actions to alternate site(s).

vi. Plan administration, maintenance, and exercises.

CHAPTER 5. Glossary of Terms, Abbreviations, and Acronyms

Continuity of Operations - Term used to denote the need for an organization to operate effectively during a crisis or emergency event.

Delegations of Authority (DOA) - Official NASA document or documents delegating authority from one individual to another with respect to taking certain actions to ensure continuity of operations.

Executive Order (EO) - Official Executive Office of the President (EOP) documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

Federal Preparedness Circular (FPC) - Official Federal Emergency Management Agency (FEMA) documents which are intended to direct, guide, inform, and instruct Federal agencies in meeting Federal and agency emergency preparedness and response requirements.

National Response Plan - National level emergency response plan which outlines the overall emergency response responsibilities of all Federal Government agencies, State, and local government agencies, and other supporting activities.

Functional Activities Listing - Official NASA organization document that outlines the functions the organization performs in support of its mission.

Interdependency - Used in the context of the MEI program: Any asset on which an MEI is dependent; NASA or other Agency-owned or -operated, that the MEI depends on or is depended on, to perform its mission (e.g., power, communications, facility, other utilities).

Mission Essential Infrastructure (MEI) - Operations, functions, physical assets, IT resources deemed by the Agency to constitute the Agency's most critical and essential to the success of NASA's mission. Established in PDD 63, "Critical Infrastructure Protection."

Mission Statement - Official NASA organization document, which establishes the mission (purpose) of the organization.

NASA COOP Criteria - Information established to guide NASA organizations in determining the criticality of NASA operations and functions as they relate to the need to ensure that select operations and functions can continue to operate under emergency situations.

NASA Senior Management - NASA personnel in designated management or supervisory positions, generally at the Administrator, Enterprise, Center Director level (e.g., Directorate, Division, Branch).

Plans of Succession - Official NASA documentation outlining processes and procedures, and identification of individuals designated as having authority to succeed.

Presidential Decision Directive (PDD) - Official Executive Office of the President (EOP) documents whereby the President of the United States promulgates decisions and establishes requirements on national security matters.

Vital Records - essential agency records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).

APPENDIX A. IT Systems Criticality Questionnaire

A.1. General

a. A key aspect in the continuity of operations planning process is to identify what operations and functions, IT supporting systems, if any, are performing critical functions and to determine how critical these functions are to the overall mission.

b. Information sensitivity and criticality are not the same.

c. Not all IT operations are critical or critical 100 percent of the time.

d. An effective Continuity of Operations Plan will allow for these situations by identifying all IT operations, establishing criticality criteria, and then prioritizing the operations and supporting IT systems. Only the most critical operations (i.e., mission-essential operations) and their supporting facilities and IT system(s), are considered in continuity of operations planning.

A.2. Procedures

Sample forms for accomplishing the following procedures are attached as Tabs A, B, and C to this appendix.

A.2.1. Mission Statement.
Enter the office mission statement provided by the senior official responsible for the overall operations of the affected office. (See Tab A.) Remember, this is a general mission statement, not a listing of office operations, i.e., why does this office exist?

A.2.2. Functional Activities Listing.
List all of the functional activities, as identified by the senior office official and key end-users that the office performs to accomplish the mission. (See Tab A.) Ensure that all operations are listed and a record of IT support and other special requirements is developed.

A.2.3. Criticality Matrix.
Development of the criticality matrix is a two-part process.

First, determine why any of the office operations are critical.

List key criticality factors or guidelines developed by the senior office official.

Enter each function and supporting system, identified in the Functional Activities Listing, next to the appropriate criticality factor.

Determine, in terms of time (minutes, hours, days), how long the system supporting that function can be "out-of-service" before mission failure occurs.

If there are a number of similar operations and systems for the same factor, consider weighing the factors. The total weights will determine the priority order of factors. The priority order of operations will be determined by the timeframes in which each must be re-established. Use the Criticality Factors and Timeframes Matrix at Tab B to assist in determining function criticality.

Second, using the information developed from the Criticality Factors and Timeframes Matrix at Tab B, develop the final Office Function Criticality Matrix (See Tab C.) Enter individual operations in descending priority order, based on their criticality timeframes. In an IT environment, it is necessary to account for less-than-catastrophic situations. Therefore, the timeframes of the loss, damage, or destruction of data and/or hardware must be considered separately.

Third, determine which of the critical operations are absolutely essential to accomplishing the office mission. These operations and systems will be the only ones supported under the Continuity of Operations Plan.

TAB A

OFFICE MISSION AND FUNCTIONALITY MATRIX

MISSION STATEMENT:								
Functional Activity	IT Support Required?		IT Dependency Level (%)				Special Requirements	
	YES	NO	0-25	26-50	51-75	76-100	Sensitive Y/N)	Periodic (Time)

TAB B

CRITICALITY FACTORS AND TIMEFRAMES MATRIX

CRITICALITY FACTORS AND TIMEFRAMES							
FACTOR	FUNCTION	TIMEFRAME					
IMMEDIATE	SHORT TERM	MEDIUM TERM	LONG TERM	CONTINUOUS	PERIODIC		

TAB C

OFFICE FUNCTION CRITCALITY MATRIX

FUNCTION CRITICALITY MATRIX

Functional System/ Application	Criticality			Adverse Situation (Data/ Hardware)
HIGH <- Hrs*	**MEDIUM** - Hrs *	**LOW** > Hrs*		
				Lost
			Damaged	
			Destroyed	
				Lost
			Damaged	
			Destroyed	
				Lost
			Damaged	
			Destroyed	
				Lost
			Damaged	
			Destroyed	

APPENDIX B. Critical Resources Inventory Outline

B.1 General

a. The Continuity of Operations Plan must provide for the reestablishment of only those office assets absolutely necessary to support critical and essential operations.

b. Determining the specific resource requirements begins with a critical review of existing resources.

c. Following the inventory, the COOP planner, office senior official, and key end-users must determine the minimum resources required to establish a viable, effective office in an alternate location for an undetermined period of time.

B.2 Inventory Procedures

There is no specific format for developing a critical resources inventory. In terms of physical property, existing property inventories provide most, but not all, of the information required. There are key items of information that must be included in the resources inventory:

B.2.1 Facilities.

The inventory must specify the current location(s) of all office operations and the minimum floor space required. (NOTE: COOP site floor space will not equal existing floor space, but must provide for the minimum essential requirement.) If the office receives routine support from other activities within the same organization and/or Center (e.g. copier support, mailroom) that will be required but will not be readily available, provisions for obtaining this support must be taken into account.

B.2.2 Hardware.

The inventory must provide a full description of all IT hardware and peripherals, a specific location, and a description of any special features or requirements. If known, the inventory should also provide replacement cost or original purchase and lease cost. Finally, the inventory must indicate the criticality factor and timeframe for each item, as well as the replacement source.

B.2.3 Software and Applications.

The inventory must provide a full description of all IT operating system software and applications, specific location(s)/systems, the individual responsible for the software, use or list of operations supported, source, replacement cost, and a description of backup procedures and backup storage locations. The inventory must also indicate the criticality factor and timeframe for each item.

B.2.4 Vital Records and Databases.

The inventory must provide identifying information on each vital record or database, specify the owner and/or individual responsible, describe backup procedures and locations, and describe its use(s) and application(s) supported. The inventory must also indicate the criticality factor and timeframe for each item.

B.2.5 Communications.

The inventory must fully identify all communications networks (e.g., line identifiers, condition types, speed, types and periods of service, protocols, protection features, connectivity, and vendor). It must also indicate criticality and timeframe for each circuit.

B.2.6 Environmental and Utilities Support.

The inventory must identify and describe special environmental support equipment, all utilities connectivity to include backup and UPS power, and any special physical security provisions that are critical to essential operations. The description should also include technical specifications, identification of vendor, replacement cost and time (if known), and indicate criticality in terms of IT hardware support requirements.

B.2.7 Furnishings.

The inventory must specify the type and quantity of required furnishings. (NOTE: Furnishings should be kept to the absolute minimum in terms of quantity and type.) It must identify replacement vendor(s) and cost and time (if known).

B.2.8 Supplies and Forms.

Special IT supplies and forms, as well as a limited quantity must be identified in the inventory. The inventory should also describe the use of any special supplies and forms, identify the responsible individual, the location of both normal operating stocks and backup supply, description of the item, and vendor or resupplier.

B.2.9 Technical and Maintenance Support.

The inventory must identify special technical and maintenance support minimum requirements, identify suppliers, identify and describe existing support agreements, and/or describe procedures and responsible individuals for obtaining needed support.

B.2.10 Personnel.

Personnel are not normally listed in a resources inventory except in terms of staffing requirements. In developing a COOP, staffing should be kept to the absolute minimum necessary to perform essential operations. Include appropriate physical security requirements. Key individuals are identified by name and assigned duties as part of the continuity of operations team.
Inventory format is at the discretion of the COOP planner. However, it should detail requirements as discussed above and will be inserted into the COOP Plan as an appendix or annex. Provided below is an example of inventory worksheets.

Sample Inventory Worksheets

Supplies Worksheet											
Item	Description	Color	Model/Serial Number	Unit **Cost**	Qty **1**	Qty **2**	Qty **3**	Qty **4**	Qty **5**	Total **Needed**	Total **Cost**
										0	$

Software Requirements Worksheet								
Make	Version	Unit Cost	**Qty 1**	Qty 2	Qty 3	Qty 4	Qty 5	**Total Needed**	**Total Cost**
								0	$

Hardware Requirements Worksheet									
Make	Model	Unit **Cost**	Qty **1**	Qty **2**	Qty **3**	Qty **4**	Qty **5**	**Total Needed**	**Total Cost**
								0	$

APPENDIX C. Sample Continuity of Operations Plan Format

Sample Cover Sheet

National Aeronautics and Space Administration

Office of XXXXXXXX

Johnson Space Center

Houston, Texas

Continuity of Operations Plan

For

[[[[[[Operation/Function Name]]]]]]

Copy ___of ___Copies

Table of Contents

6. COOP Activation

7. Roles and Responsibilities

a. Management

b. Continuity Teams

8. Training and Testing COOP Capability

9. Plan Maintenance

10. Delegations of Authority

11. Plans of Succession

12. Vital Records

13. Plan Implementation (Action Plan)

a. Notifications Process

b. COOP Team Tasks

c. Initial Emergency Response

d. Resumption Activity Processes and Procedures

e. Recovery Activity Processes and Procedures

f. Restoration Activity Processes and Procedures

g. Reporting Structure

h. Safety

i. Security

14. Mutual Aid Support Agreements

a. Interagency

b. Intra-Agency

Appendices:

A: IT System Criticality Questionnaire

B: Critical Resources Inventory

C: Supplies, Equipment Resources Inventory

D: Continuity Team Designations, Names and Contact Information

E: Vendor Contact Information

F: Vital Records Inventory

G: Off-site Storage Locations w/Maps and Directions

H: Established IT System Contingency Plans